Architecture and Assessment: Privacy Preserving Biometrically Secured Electronic Documents

Prepared by:
David Bissessar
Dong Liu
Sherine Nahmias
Canada Border Services Agency
14 Colonnade Road, 2nd Floor Ottawa, Ontario

John Harvey
Carleton University
1125 Colonel By Drive
Ottawa, Ontario

Scientific Authority:
Paul Hubbard
DRDC Centre for Security Science
613-992-0595

Contract#CSSP-2013-CD-1064

IMPORTANT INFORMATIVE STATEMENTS

Science and Engineering Directorate

Border Technology Division

Division Report 2014-45 (TR)
November 2014

Architecture and Assessment:
Privacy Preserving Biometrically
Secured Electronic Documents

Authors:

David Bissessar

Dong Liu

Sherine Nahmias

John Harvey (Carleton University)

PROTECTION • SERVICE • INTEGRITY

Canada

Dedicated to

Daniel Patrick Bissessar
March 11, 2007 – January 1, 2012

To inspiration, creativity, perseverance and happiness...
To fatherhood, love, hope, best friends, dreams, people helping
people, and doing cool things...

<u>Acknowledgement</u>

Table of contents

List of Figures

List of Tables

Executive Overview

This document explores an application which uses biometrics to secure electronic travel authorizations granted to foreign passport holders wishing to visit Canada. Rather than traditional biometrics, we use privacy enhancing techniques to derive references from the biometrics so that no biometric information must be stored by the application.

We describe the architecture and key algorithms for a biometric-enabled electronic Travel Authority (b-TA) system in which foreign passport holders obtain electronic credentials which permit entry to Canada. This b-TA can be seen as a privacy preserving biometric version of the "Electronic System for Travel Authorization" (ESTA) travel authorization required by US Customs and Border Protection (CBP) for US Visa-Exempt Countries or Canada's eTA program under Citizenship and Immigration Canada (CIC).

The b-TA application process we propose is performed online, with the applicant using a smartphone equipped with a fingerprint sensor. The issued b-TA is a cryptographically secure data package whose contents include a privacy protecting biometric identifier as well as the traveller's electronic passport (e-passport) number. The issued travel authority is stored on the smartphone and shown at later steps, when departing the country of origin and when arriving into Canada. Once verified, subsequent processing of the traveller can be streamlined by taking advantage of the biometric reference.

Our findings suggest that attribute-based credentials and privacy preserving biometric identifiers can form a basis for mobile passports (m-passports) which would be entirely paperless passports stored on the traveller's smartphone. These m-passports could include national identity document, travel authorities, and records for multiple nations.

In our current model, the verification of the biometric identifier occurs upon arriving in Canada, with a suggestion that at a greater cost, this verification could also happen when departing the country of origin. In light of this newest tragedy with Malaysia Airlines, security concerns over passport trafficking have been raised [Stastna2014]. As discussed in this report, a kiosk performing biometric verification before boarding at the country of origin can reduce use of fraudulent travel documents.

Chapter 1: Introduction

This document examines how privacy enhancing technologies could be applied to different scenarios of biometric verification which could be used within the traveller continuum for border security. As a motivating scenario, we consider the issuance and verification of biometric e-travel authorities: electronic documents (e-documents) which grant authority for foreign nationals to visit Canada.

We present the biometric-enabled electronic Travel Authority (b-TA) as an electronic document, represented by a cryptographic credential, secured to the traveller through a Renewable Biometric Reference (RBR) created from the traveller`s fingerprint, and certified by the issuer's digital signature. The b-TA is cross-referenced to the traveller's electronic passport (e-passport [ICAO9303]). This b-TA can be seen as a privacy preserving biometric version of the ESTA travel authorization required by CBP for US Visa-Exempt Countries or Canada's eTA program under CIC [CIC2014][CBP2014] . The approach we present yields benefit in terms of security, efficiency and privacy. From a security perspective, binding the cryptographic credential to the traveller through the use of biometrics prevents many types of fraudulent activity which can occur. Operational efficiency increases since automation technologies such as kiosks and electronic gates (e-gates) become possible. From the perspective of privacy, the use of RBRs removes the need to store the biometric on the smartphone. This can help alleviate public concern over the use of biometrics, and can simplify policy issues associated with privacy impact and personal information banks. The presented approach is scalable to accommodate b-TAs from multiple countries, and can lay foundations for m-passports. The document presents a general b-TA scenario, elaborates a list of security and engineering requirements, puts forward a system design, and makes an assessment of the proposed system.

Chapter 2 presents the b-TA. We discuss the main entities, operational entities, and general vulnerabilities involved in this scenario.

Chapter 3 presents the technical background, environment scan, vulnerabilities and security requirements checklist. We briefly discuss the major initiatives in the scientific and commercial arenas including current developments in the international standards community for biometric information protection.

Chapter 4 presents the selected architecture for b-TA issuance and verification, including the mechanisms for biometric enrolment and verification. We discuss the system entities, and their features. We describe the main data structures and algorithms which are important from a security and privacy point of view. We describe the triangular biometric binding which our b-TA approach implements. Furthermore we discuss possible operational efficiencies where the e-passport becomes optional after first verification. We illustrate that the proposed approach scales to become a paperless m-passport

solution. Finally, we tie the terminology used in our approach to ISO terms of biometric information protection.

Chapter 5 evaluates and assesses the selected approach in terms of the security and engineering requirements presented in Chapter 3. Assessment includes irreversibility of biometric, security of generated key, storage requirement and communication requirements. Empirical measures such as milliseconds to run will be prorated, and performance metrics may be obtained from referenced literature, since no technology demonstration will be generated from this study.

Chapter 6 concludes the document, summarizing the findings of the study, recapitulating scope and limitations, and presenting some possible next steps for ongoing work.

Chapter 2: The b-TA Scenario

This chapter aims to present the application from a technology neutral perspective to set the context for the technical solution and engineering assessment to occur subsequently. We present the b-TA scenario and discuss its general flow. We introduce the participants and protocols, and present a set of application requirements.

At its simplest, b-TA scenario consists of two transactions: *issuance*, in which the traveller applies for and is granted a b-TA, and *verification*, in which the traveller uses the travel authority to enter the country. The locations and technologies used to implement these steps may vary.
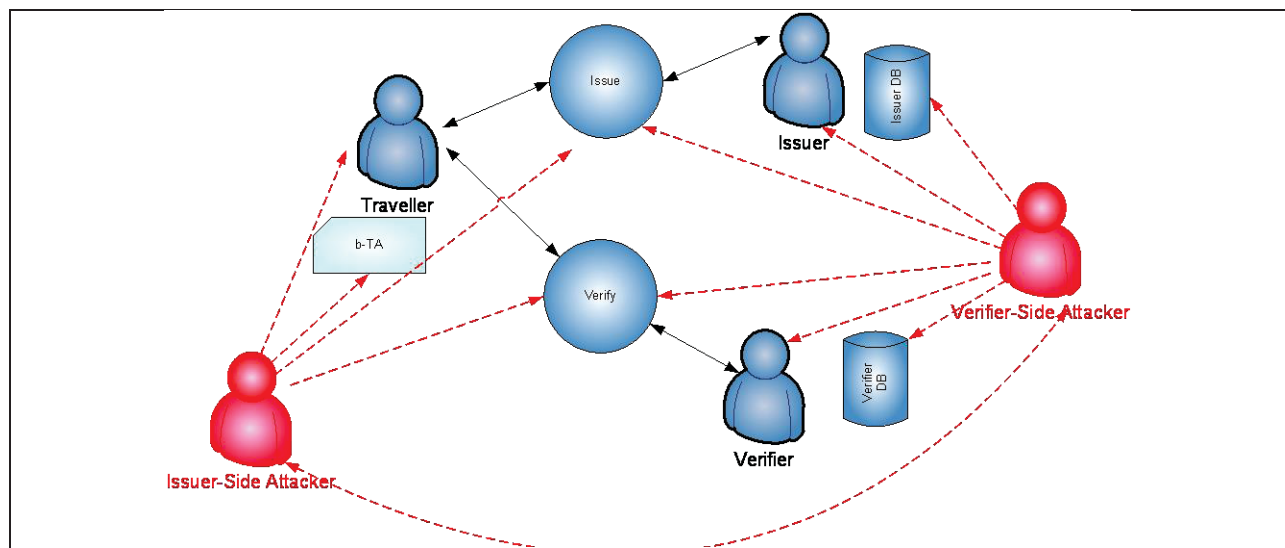
Figure 1. b-TA Context Diagram

From the perspective of biometric privacy, the b-TA scenario can be modelled as a conversation between a traveller an issuer and a verifier in which a biometrically secured document is issued and attackers attempt to compromise system security and biometric privacy.

The issuance process could take place with a paper form or with an in-person interview at an overseas government office. However, the issuance process could also take place online: from a computer connected to the internet, or via a wireless enabled device such as a smartphone. Similarly, the verification step could also occur overseas, during ticket purchase or during boarding pass issuance. It could also occur once the traveller has landed at the country of destination during border clearance procedures. A number of other travel related steps would generally occur between the b-TA issuance and verification steps. The b-TA scenario will be discussed in more detail in Chapter 4.

Main Entities, Roles, and Participants

Any number of systems and processes may be selected to implement a b-TA system. In general, the b-TA system will include three main entity types: a traveller, an issuer, and a verifier; two main processes: the *issue* process and the *verification* process; and one main data structure: the b-TA and its associated data. Through the *issue* process the issuing organization grants a b-TA to a traveller, who later presents it to a verifying organization in the *verification* process, in order to gain access to the destination country. We will discuss each of these in turn, beginning by the token that links them all: the b-TA.

The b-TA represents the credential granted to the traveller by the issuing country permitting access to the country. It can be conceptually viewed as a security printed page in a passport which represents permission to enter a country. However, in the context of this study, it is an e-document containing a number of relevant fields including biographical, biometric, and travel authorisation information which is bound to the traveller through a RBR, and rendered tamper-proof and certified by a digital signature from the issuing agency.

The b-TA will typically hold information about the traveller such as name, date of birth and passport number. It may also hold a variety of information about the permitted duration of each stay, the number of allowed entries, the validity period and the authorized purpose of travel. In an extended functionality system, the b-TA can also include annotations which might impose restrictions (such as suspension of driver's license in the home country). The b-TA can also hold cross-references to passport numbers or b-TAs of the associated family member(s).

The **traveller** in the context of this study is an individual, holding an e-passport from a foreign country, who applies for a travel authorization to visit the country of destination. In this document, the traveller has an identity (represented by biographical information, and biometric data) and a travel intent (evidenced by a destination, purpose of travel, intended number of entries, intended duration of stay). Traveller behaviour may vary significantly. Some travellers, for example, will follow protocols and operational procedures without deviating. Other travellers may actively seek to break system security by forging documents, colluding to lend documents or to buy and sell documents on the black market.

The **issuer** in this study corresponds to the government agency of the destination country that is responsible for extending visitor visas and extensions for tourists, parents or grandparents and business travellers, transit visas and necessary travel identification documents. In a Canadian context, the issuer could be Citizenship and Immigration Canada (CIC). The issuer is assumed to have system connectivity in the country of origin of the traveller. In assessing candidate alternatives, no restriction was made regarding location of service, nor was any assumption made regarding physical processes.

The role of **verifier** holds the responsibility of checking the b-TA's authenticity, and verifying ownership of the b-TA with a biometric check. This corresponds to the government agency of the destination country which is responsible for verifying the validity of b-TA and granting access to the country. In a Canadian context, the verifier could be the Canada Border Services Agency (CBSA). (Note: In more sophisticated applications, such as m-passport, discussed further, the verifier can add annotations to the traveller's document such as entry and exit stamps.)

Optional Entities

In parallel to the roles and responsibilities described above, there are a number of organizations which can be important in this scenario including the airline company and the airport authority.

Currently, for example, the **airline company** provides overseas check-in facilities and ticket issuance facilities which interface with border control systems providing advanced passenger information for incoming flights. In a b-TA system, the airline company may have a kiosk which verifies any number of conditions of the b-TA. The system proposed in this document, for example, has the airline company kiosk performing a validity check on the b-TA which may include expiry date and revocation checks.

The **airport authority** maintains security checkpoints within the international arrival airport. The airport authority is a potential user of the biometric credential carried by the traveller; however, this potential is not explored in this document.

Operational Context

In Canada and internationally there has been identified significant benefit to border security and traveller experience in extending processing of border travel information layers prior to arrival in the country of destination. As recently presented by FRONTEX to the Operational Heads of Airports Conference in Warsaw [FRONTEX2014] there is a layered approach to level of information and commitment to travel that begins overseas and progresses through the stages of travel planning to finally arrival, international travel visit and departure.
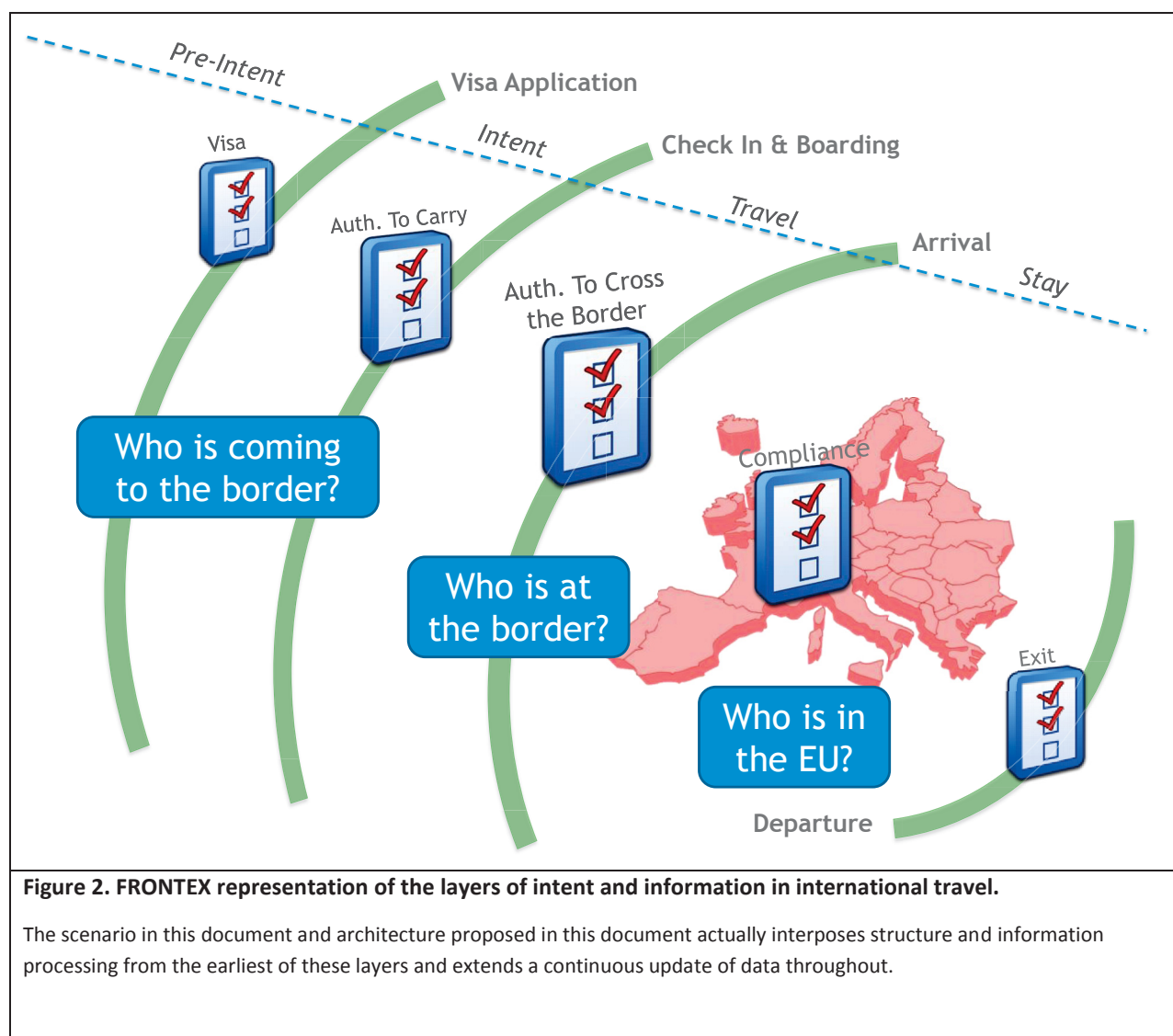
Figure 2. FRONTEX representation of the layers of intent and information in international travel.

The scenario in this document and architecture proposed in this document actually interposes structure and information processing from the earliest of these layers and extends a continuous update of data throughout.

As modelled in the diagram of Figure 2, and provided by FRONTEX [Zoy2014][FRONTEX2014], a number of decisions and an increasing level of passenger travel intent information occurs along the traveller continuum which suggests a layered approach to border management. The application for travel authority (or travel visa in the above diagram) is the initial point at which possible intent (a "pre-intent") to travel is communicated. Air ticket purchase solidifies this intention. At the time of Airport check-in, "intent" now transitions to "travel". In-transit the travel is committed: the traveller has departed the country of origin and is approaching the border. Arrival at destination occurs at the border: a kiosk performs traveller identity check, document verification, and also records the customs declaration. After approval of the traveller's request for entry at the border, an entry record may be created. The traveller can then visit the country domestically. On departure, an exit record may be created.

The technologies presented in this document intercede at important stages in this process, with the b-TA occurring overseas (where the FRONTEX diagram in Figure 2 shows a Visa application): b-TA application, airline check-in, border verification. Our technologies can extend to entry and exit recording and reconciliation.

General Vulnerabilities

Regardless of which approach is chosen to implement the b-TA system, there are a number of general vulnerabilities which must be considered when assessing a candidate system's security and biometric privacy.

If the travel document is not bound to the individual through biometrics a number of problems can occur, for example, can the travel document transferred to another traveller? From the perspective of user privacy, if the database in which biometric information is stored becomes compromised, can the biometric itself be stolen and reused? This leads us to another security concern – if a database and associated biometric information has been compromised, does this further enable fraudulent access into the system?

As illustrated in Figure 1, the entities, databases, processes and communications channels which make up a system are all susceptible to attack. Categorizing attacks in terms of whether they occur using client-side resources or server-side resources may be helpful. A client-side attack could be an attempt to modify an issued credential to gain unauthorized access. A server-side attack could consist of examining the databases of the issuer and verifier to reverse engineer an individual's biometric. These could also serve to illustrate the possibility of mounting one attack in terms of another: by using a reverse engineered biometric as input to a client-side attack to create a fraudulent credential using a fake biometric. These and other vulnerabilities will be discussed in Chapter 3.

These must be addressed by any candidate solution to the b-TA scenario.

Chapter 3: Technical Background and Environment Scan

Technical Background

Pedersen Commitments

The Pedersen commitment [Ped92][Dam99] allows a sender to create a publically storable commitment on a value which irrefutably binds to the value, and also perfectly hides the value from being derived.

The Pedersen commitment scheme has two protocols $C_s = \mathrm{Commit}(s, r) = g^s h^r \pmod{p}$ and $(s, r) = \mathrm{Open}(C_s)$ where g and h are publically known algorithm parameters, generators of group Z_q, where the secret s is a value from Z_q and random value r is also secret and uniformly drawn from group Z_q. The specification of mod p for Pedersen commitments will be omitted throughout this report but should be clear from context.

In the protocol presented in this report, Pedersen commitments are used to commit to the biometrically derived cryptographic key: the "hiding" property preserves privacy of the key, and the "binding" property ensures security.

Digital Signatures

A digital signature is a mathematical scheme for securing and demonstrating the authenticity of a digital message or document [Gol04]. A valid digital signature gives recipient assurances that the message was created by a known sender (authentication), and that the message has integrity (was not tampered with). It also supports the non-repudiation property (the sender cannot later deny having sent the message). Digital signatures are used in the protocols we propose to seal the attributes provided by the traveller into an electronic travel document signed by the issuing authority.

Proofs of Knowledge

A Proof of Knowledge (PoK) is an interactive protocol in which a prover P convinces a verifier V of possession of particular knowledge, without divulging that knowledge [Gol01]. In general, a PoK has the properties of completeness and validity. The property of completeness states that if P holds the required knowledge, P will succeed in convincing the verifier V of that fact. The property of validity states that if verifier V accepts the proof, P really knows the required knowledge. An additional property can be added: zero-knowledge, which states that during the protocol, V learns nothing beyond the fact that P holds the required knowledge. A PoK holding completeness, validity, and zero-knowledge is called a Zero Knowledge Proof of Knowledge (ZKPoK) [Gol01].

Secure Sketches and Fuzzy Extractors

A fuzzy extractor is a pair of algorithms ($\mathrm{gen}(...)$ and $, \mathrm{rep}\,(...)$) which allows one to extract randomness from an input string and later reproduce that randomness exactly using another input string sufficiently close to the original input string. Most fuzzy extractor schemes also produce helper data which is created during the initial generation step, and used to assist in reproducing the randomness. The pair of algorithms can be represented as

$$< P, R > = gen(b) \quad \text{and} = rep(b', P)$$, where:

P is public data safe for storage, used to assist in the $\mathrm{rep}(...)$ algorithm,
R is a random string that can be used for cryptographic purposes,
b is an input string, for example a biometric template, and
b' is another input string within a certain similarity distance from the original string.

Fuzzy extractors have clear applications in the field of biometrics, with specific algorithms for different biometric modalities. For more background into fuzzy extractors see [JW99] [JS02][DRS04]. Some vulnerabilities are explored in [Sto09][Boy04][SB07]. For some algorithms on specific biometric modalities, please see [Kev05][USJ05].

Attribute-based Credentials

Various attribute-based credential (ABCs) systems have been proposed in the literature; however, two of the predominant ones today are digital credentials and anonymous credentials. We discuss these at a high level and attempt to highlight the important similarities and differences.

In general, a cryptographic credential system includes three entities: the individual, the issuer, and the verifier. The individual applies for a credential from the issuer by submitting attributes. The individual receives a signed data package which is shown later to a verifier to claim a privilege.

Anonymous credentials and digital credentials are similar in some ways. The general protocol proceeds as follows:

1) An *issue* protocol, in which:

    a. User U sends attributes X to Issuing organization I

    b. I issues credential C to U

2) A *show* protocol, in which:

    a. U presents C for verification of signature

    b. U makes a claim involving attributes of X and proves it to the verifier to claim a privilege

However, the schemes differ in some important manners, including:

1) Anonymous credentials explicitly include the concept of pseudonyms, whereas digital credentials do not.

2) In the *show* protocol of anonymous credentials, U does not show the values of the attributes X to verifier V, but rather uses a ZKPoK. This provides additional privacy in a multiple-show scenario.

Environment Scan

In this section we briefly review the current literature and highlight the most promising solutions. We focus on the use of privacy-enhancing biometric technologies (PETs) specifically for electronic authentication.

The concept of a privacy-enhancing biometric is a relatively recent one, and the field is rapidly advancing. There are several consequences of this immaturity that make it difficult to make a critical comparison of the many proposed protocols and implementations, including but not limited to:

- lack of a common notation for the various cryptographic primitives and protocols;
- lack of a common framework for security and privacy assessment.

We will, where possible, indicate correspondences between the terminologies via footnotes when they are not clear from the context.

Literature Overview

Privacy Enhancing Techniques for Biometrics

A number of techniques have been proposed to help fulfill biometric use cases of enrolment, verification and identification. Some thorough surveys of the fields of biometric encryption (BE) have been published including studies by Rathged and Uhl [RU11], Dodis et al. [DRS08] and Thieme et al. [PSTP351] . We provide an overview of some important developments within this area.

Important first steps in the privacy preserving use of biometrics include a system proposed by Davida et al. which presents an architecture for an offline database and a card-based biometric matching system which used encryption and matching to protect biometric templates [DFM98]. In 1998 Soutar et al. [Sou98] proposed an image-based approach which using a majority vote algorithm and Fourier transforms. Originally dubbed "Biometric Encryption" this approach has become known in the literature as "Mytec" (after the company who commercialized it).

In 1999, Juels and Wattenberg [JW99] presented a new cryptographic primitive called the fuzzy commitment, which would form the foundation of an important area of research. The fuzzy extractor offers the ability to create a commitment on a secret which can be unlocked with a witness that is sufficiently close to the original secret relative to a vector distance metric. In 2002, Juels and Sudan [JS02] introduced the fuzzy vault which offered similar functionality to the fuzzy commitment but was based on a set difference metric rather than a vector difference. In 2004, Dodis et al. [DRS04] generalized the fuzzy commitments and fuzzy vaults put forward in [JW99] [JS02], presenting two corresponding primitives, the Fuzzy Extractor (FE) and the Secure Sketch (SS). In 2004, Boyen [Boy04] pointed out vulnerabilities in FE and SS under scenarios in which multiple enrolments can yield information which can be used to

deduce the biometric. In 2007, Sheirer and Boult [SB07] described a number of possible attacks on biometric encryption and fuzzy vaults. They also presented general requirements for biometric encryption and privacy enhancing technologies which guards against the types of attacks put forward in their paper. In 2009, Simoens, Tuyls and Preneel [SKTP09] further examined attacks on SS in multiple use scenarios introducing security definitions for indistinguishability and reversibility.

While we have presented fuzzy extractors in some detail, other promising techniques have been proposed. Some of these include quantized index modulation [LT03], biometric key generation [Bal08], and techniques based on on the merger of cryptographic protocols (e.g., using homomorphic encryption) and fuzzy extractors [Sto10].

Privacy-preserving techniques have been applied to specific biometric modalities. Hao, Anderson and Daugman [HAD06] published a fuzzy extractor approach for iris templates. Bringer et al. [Bri07] further studied the approach presented in [HAD06]. Approaches specific to fingerprints include Clancy et al. [CKL03] and Nagar et al. [NNJ08] who propose fuzzy vault-based approaches. A number of biometric encryption algorithms have also been proposed for facial recognition including Mytec (mentioned previously), an image processing technique by Savvides [Sav04] and a fuzzy extractor approach by Sutku et al, [Sut09].

As will be discussed later in this section, a number of vulnerabilities have been identified in the literature. Referring to Stoianov, [Sto10] these include "Inverting the hash"; "False Acceptance (FAR) attack"; "Hill Climbing attack" [Adl04]; "Nearest Impostors attack" [Sto09] ; "Running Error Correcting Code (ECC) in a soft decoding and/or erasure mode" [Sto09]; "ECC Histogram attack" [Sto09]; "Non-randomness attack against Fuzzy Vault" [CST06]; "Non-randomness attack against Mytec2 and Fuzzy Commitment schemes" [Sto09]; "Re-usability attack [SB07][Boy04]; Blended Substitution attack [SB07]; and Linkage attack [CS09]. Stoianov presents a detailed description details of these vulnerabilities and an analysis in the context of the Mytec, fuzzy commitment and fuzzy vault biometric encryption schemes.

Credential Systems

We introduce some previous work in the area of credential systems and highlight the applicable approaches to non-transferability and their weaknesses. In 1985, Chaum [Cha85] identified the privacy concerns resulting from the ability of service providers to aggregate electronic records and presents a pseudonymous system whose security is based on the discrete logarithm problem and blind signatures. Credentials in this system can be copied and transferred. In 1986, Chaum and Evertse [CE86] generalized the system presented in [Cha85] to accommodate multiple credentials, from different issuers and verifiers. Following this, Dåmgard [Dam88] and Chen [Che96] presented alternative approaches, also including a Trusted Third Party (TTP). Canetti et al. [Can07] proposed a non-transferable anonymous credential scheme which was patented to IBM in 2007 as US Patent #7222362. In Canetti's

approach to non-transferability, along with the credential, the user is issued a master-key that is bound to a valuable piece of personal data which the individual is reluctant to share (such as a bank account number). To claim the privilege granted by the credential, the user must prove knowledge of the master key. However since the master key is too valuable to share, no unauthorized users are presumed to know it. As stated by the authors, this approach to non-transferability does not prevent sharing, but rather dissuades it. In 1999, Lysyanskaya et al. [LRSW99] presented an anonymous credential system which, similarly to Canetti's approach, dissuades by relying on the user's motivation to preserve a high-value secret. In 2000, Brands [Bra00] presented the digital credentials scheme, a single-show credential system. In this scheme, the credential is provided to the verifier, and the specific attributes used are divulged during the Show protocol. Brands provided a non-transferability approach of embedding a biometric into the credential. This does not provide biometric privacy, since the biometric itself must be used and divulged. In 2001, Camenisch and Lysyanskaya [CL01] presented "Anonymous Credentials", a credential system using ZKPoK to deliver multi-show credentials. These approaches all have similar weaknesses: either a trusted third party is used, or if any non-transferability is present it relies on a disincentive approach which can be circumvented if colluding users have no qualms about sharing secrets.

International standards and working groups

International Organization for Standardization (ISO)

The ISO includes a number of relevant technical committees, in particular:

- ISO/IEC JTC 1/SC 37 *Biometrics*
- ISO/IEC JTC 1/SC 17 *Cards and personal identification*, which includes application of biometric technologies to cards and personal identification
- ISO/IEC JTC 1/SC 27 *IT Security techniques*, which covers biometric data protections techniques, biometric security testing, evaluations, and evaluations methodologies.

From those technical committees, the following current or draft documents are of specific interest for the b-TA scenario:

- ISO/IEC PDTR 29195 *Traveler processes for biometric recognition in automated border control systems* [ISO13] considers the operational environment and vulnerabilities specific to a traveller processing scenario, with technical focus on both face and fingerprint biometric modalities. There is currently little discussion of the security of the underlying cryptographic primitives.
- ISO/IEC WD 30136 *Performance Testing of Template Protection Schemes* [ISO13b] presents a generalized architecture for biometric access control, and gives a detailed assessment of

attack vectors and performance metrics, including single- and multi-system Successful Attack Rate (SAR) and privacy leakage. Revocability and unlinkability are also discussed. We draw on this reference for some aspects of the "Vulnerabilities" and 'Security and Engineering Checklist'.

- ISO/IEC 24745:2011(E) *Biometric information protection* [ISO11] provides guidance for the protection of biometric information under requirements for confidentiality, integrity and renewability/revocability during storage and transfer. We draw on the ISO 24745 document extensively in the determination of our selected approach in Chapter 4.

European Union PRIME / PRIMELife, ABC4Trust

The EU PRIME (Privacy and Identity Management for Europe) and its follow-on PrimeLife ran from 2006 - 2008 and from 2009 - 2011 respectively, bringing together industry (including IBM research GmbH CH, Europäisches Microsoft Innovations Center GmbH DE, SAP AG) and academia (Technische Universität Dresden DE, Karlstads Universitet SE).

The focus of PRIME was to develop mechanisms for managing multiple identities safely across different contexts, by allowing a user to establish provable credentials without necessarily revealing identifying information. PrimeLife built on that, with a deeper focus on the fundamentals of privacy-enhancing identity management , and its particular application to web-based interfaces and services.

In particular, the *Final report on mechanisms* from PrimeLife work package WP2 [SAM11] discusses modified Boneh-Boyen signatures, zero-knowledge proofs and Σ-protocols, and credential signature schemes in the context of an "oblivious transfer with access control" protocol, by means of which a group of pseudonymous users may obtain access credentials to a database from an issuer. They present a detailed construction based on an extension of the work of Camenisch [CDN10b], including issuer and database setup, and issue and transfer protocols.

The PrimeLife *Final report on mechanisms* also contains a case study for a mechanism supporting users' privacy and trust.

The ABC4Trust Project

Following Primelife, the European Union launched the ABC4Trust project [ABC4Trust]. In the context of the project name ABC stands for Attribute-based credentials. This Project aims demonstrate the interoperability of ABC systems – Microsoft UProve and IBM IDEMIX. The project includes a demonstration of the systems and their interoperability in a university setting. To our knowledge the project does not include a component to tie the credential to the user's identity through either biometrics or biometric encryption.

<u>The AU4EU Project</u>

The AU4EU project builds on ABC4Trust and is funded under the Seventh Framework Programme (FP7). The aim of the AU2EU project is to implement and demonstrate in a real-life environment an integrated eAuthentication and eAuthorisation framework to enable trusted collaborations and delivery of services across different organisational/governmental jurisdictions. Our research is applicable in the area of inter-government and cross-jurisdictional services. Both areas in which the subject area in our research is relevant. The AU4EU project budget is 8.6M Euro.

<u>European Union TURBINE Project</u>

TURBINE (TrUsted Revocable Biometric IdeNtitiEs) is a research project awarded 6.3 million Euro funding by the European Union under the FP7 for Research and Technology Development. Running from 2008 - 2011, TURBINE aimed to develop innovative digital identity solutions, combining:

- secure, automatic user identification thanks to electronic fingerprint authentication
- reliable protection of the biometrics data through advanced cryptography technology

This program brought together industry (including Philips Research Europe, Morpho) and academia (K.U. Leuven, Gjøvik University College, University of Twente), and focused on fingerprint as the biometric modality of choice, addressing specifically:

- application of cryptographic techniques to fingerprint biometrics to obtain a non-invertible and protected pseudo-identity bit-string for enrolment and subsequent verification
- multiple re-generation of independent unique bit-strings based on the same fingerprint
- revocable and multiple pseudo-identity management scheme based on these unique bit-strings
- highly reliable biometric fingerprint 1:1 secure verifications using these unique bit-strings
- multi-vendor interoperability of these unique bit-strings
- detailed verification performance analysis, evaluated against very large public and private fingerprint databases
- comprehensive risk analysis and system security
- contribution to developing international standards for biometric template protection

National Studies, Standards and Recommendations

US National Institute of Standards and Technology (NIST)

   The United States National Institute of Standards and Technology (NIST) is active in the area of biometrics and information security. In a 2011 Special Publication *Electronic Authentication Guideline* [NIST11], technical recommendations to national agencies, supplementing an earlier Memorandum *E-Authentication Guidance for Federal Agencies* [OMB M-04-04], are presented. These two documents outline a high-level process based on determining an appropriate assurance level based on an operational risk assessment, and then choosing and validating an electronic authentication technology against the requirements for the chosen assurance level. Probably the most appropriate level for the b-TA scenario under discussion here is NIST Level 2, described as

> […] *provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. For single factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One-Time Password Devices are allowed at Level 2. Level 2 also permits any of the token methods of Levels 3 or 4. Successful authentication requires that the Claimant[1] prove through a secure authentication protocol that he or she controls the token. Online guessing, replay, session hijacking, and eavesdropping attacks are resisted. Protocols are also required to be at least weakly resistant to man-in-the middle attacks* […]

   Minimum entropy requirements are given for each of the assurance levels; although specific biometric implementations are not discussed, it is feasible to map these requirements into various biometric modalities using information theoretic treatments found in the biometrics research literature. Credential management (including binding and credential storage) and credential renewal, re-issuance, and revocation are discussed. We draw on this reference for many aspects of the "Vulnerabilities" and "Security and Engineering Checklist".

BioKeyS III-Final Report

   A recent report from the Bundesamt für Sicherheit in der Informationstechnik[2] [Bund11] describes a practical implementation of a Biometric Encryption (BE) scheme based on Juels and Wattenburg's fuzzy commitment scheme. Security and privacy of the scheme are discussed, and the authors identify the former as insertion vulnerabilities and the latter as eavesdropping vulnerabilities. Assuming a trusted

---

[1] In the context of an b-TA document, the term *Claimant* may be read as *traveller, who claims the privilege of entry into the country during the verification step.*
[2] English: *Federal Office for Information Security*

enrollment environment, they define a Perfectly Private Biometric (PPB) system as one that outputs the minimal amount of information necessary for identification or verification[3] (i.e., a binary accept/reject decision). By extension, they describe a Perfectly Private Biometric Encryption (PPBE) system as one from which it is impossible to extract any biometric information, apart from the binary accept/reject decision. Depending on the application, a positive decision may take the form of the release of a conventional cryptographic key, which is then used to gain access to private (non-biometric) data. Parallels are drawn with cryptographically hashed passwords; only a one-way transformed version of the biometric witness value (password) is stored; and compared to a candidate value via the same one-way function. The authors draw extensively on the terminology and primitives described in [ISO11].

The resulting BioHASH® system develops a number of operationally interesting enhancements including a hardware binding scheme that makes use of an application specific identifier (AID) to improve unlinkability; several fusion schemes that allow for combinations of multiple biometrics (possibly of different modalities); and a privacy bootstrapping architecture that allows a third-party non-privacy-preserving template generation storage and comparison system to be "wrapped" in the secure, privacy-preserving commitment scheme - the resulting scheme thereby benefiting from the possibly superior classification (DET) performance of the third-party classifier compared to the intrinsically limited Hamming classification performance of the underlying fuzzy commitment scheme (FCS).

The classification performance of the BioHASH® SDK was investigated extensively using both publically available fingerprint image data from the Spanish Ministerio de Ciencia y Tecnología[4] (MCYT) and a proprietary FingerQS database from Secunet Security Networks AG, and an attempt is made to assess the privacy (information leakage) performance via the distribution of Hamming distance of the binary representation of the minutiae templates.

CSS PSTP-02-351 BIOM

IN 2010, the Public Security Technical Program (PSTP) of Defence Research and Development Canada's (DRDC) Center for Security Sciences (CSS) funded a project, PSTP-02-351 BIOM, which researched the vulnerabilities of biometric data. The Study Team for PSTP-02-351 BIOM conducted a survey and evaluation of Biometric Data Safeguarding Technologies. To address the Community of Practice (CoP) objective of evaluating, analyzing, and implementing biometric technologies that enhance national capabilities in access control, identity verification, and e-Commerce security.

The lead federal department for the study was the Canada Border Services Agency (CBSA). The primary author of the report was International Biometric Group (IBG). Additional partners included DRDC

---

[3] A verification system consists of a claim of identity plus a 1:1 comparison, whereas an identification system involves a 1:many comparison with no explicit claim of identity. As such, verification systems typically impose less onerous requirements on a system's detection error performance.
[4] English: Ministry of Science and Technology

– Toronto, the Office of the Information and Privacy Commissioner of Ontario (IPC), the Royal Canadian Mounted Police (RCMP), Transport Canada (TC), Indiana University-Purdue University Indianapolis (IUPUI), and University of Toronto.

The study team surveyed typical applications in which biometric data is safeguarded; analyzed privacy-enhancing technologies (PETs); conducted a comparative study of iris recognition using several iris image datasets of varying quality; analyzed factors that can complicate the use of iris recognition as a PET; and tested a commercial, fingerprint-based PET to assess its utility as a data safeguarding technology.

The Team developed novel methodologies to survey and compare biometric PETs of varying maturity and technology readiness level (TRLs). Results showed that although the commercial landscape of biometric PETs is limited, a wide range of PETs have been developed whose viability for real-world applications varies. Iris recognition shows considerable promise as a potential PET due to its low false match (i.e., impostor) rates. Commercial fingerprint PET performance was, at certain thresholds, roughly equivalent to that of a widely-utilized fingerprint algorithm. Results demonstrate that biometric PETs, when deployed in suitable applications and implemented in a considered fashion, are viable solutions for biometric data safeguarding.

The study included an extensive literature review of privacy enhancing techniques applicable to biometrics which included the fuzzy extractors used in this study.

ISO Terminology and Architectures

Before we describe our selected approach, we establish some terminology. Given the range of terms used in the domain, we choose to follow ISO standard 24745 [ISO11].

The concept of a RBR is described in Annex C of the 24745 standard as follows:

" *Renewable biometric references (RBRs) are revocable / renewable identifiers that represent an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from a captured biometric sample. A renewable biometric reference does not allow access to the original biometric measurement data, biometric template or true identity of its owner. Furthermore, the renewable biometric reference has no meaning outside the service domain.*"

In particular, the ISO document distinguishes between an RBR and a Biometric Reference (BR) - which does not intrinsically protect the Personally Identifiable Information (PII) of its owner, and therefore must be protected by other means such as conventional cryptographically-secure transmission and storage. The essential elements of an ISO RBR are as follows:

Enrolment process:

- a *Pseudonymous Identifier Encoder* (PIE) that takes the extracted biometric feature data and produces

- a *Pseudonymous Identifier* (PI) that may safely be stored and/or transmitted without exposing the user's PII, together with

- some *Auxiliary Data* (AD) used in the generation of the PI from the extracted biometric features

- an *Identity Reference* (IR) that contains non-biometric personal data specific to the domain or realm of the particular identity management system (IdMS) such as name, social security number etc.

- a *Common Identifier* (CI) that may be used to connect a non-biometric IR to a person's biometric record (BR) in the case that these are not co-located: this might be a unique user identifier (UUID) string for example.

Verification process:

- a *Pseudonymous Identifier Recorder* (PIR) that takes the extracted biometric feature data, usually together with some auxiliary data[5], and produces

- a *Pseudonymous Identifier* candidate (PI*) that will be used for comparison with the stored PI

- a *Pseudonymous Identifier Comparator* (PIC) that compares the candidate identifier PI* to the stored PI and outputs an accept/reject identity verification decision.

The AD and its relationship to the PI is the most difficult of these elements to grasp since its composition is dependent on the particular RBR architecture and underlying cryptographic primitive. At its simplest, the AD might contain information used to ensure repeatability of the extraction of biometric features. For example, in the case of a fingerprint-based RBR it might consist of presentation alignment information. However in most cases of practical interest, the AD-PI relationship will be more complex. For example, in the context of Juels and Wattenburg's original biometric fuzzy commitment scheme, the AD will include a Hamming distance[6] derived from the biometric input data using the so-called code-offset construction [JW99], while the PI is a simple cryptographic hash. In the context of a Bio-token scheme [BSW07] it is the PI that is biometrically-derived while the AD is purely cryptographic (see Table D.1 of [ISO11]).

The ISO 24745 standard describes the application of these RBR elements within a number of possible IdMS architectural models:

---

[5] Auxiliary data: The standard gives at least one method ("Extended PIR") that does not require auxiliary data

[6] Hamming distance is a measure of distance between two equal-length symbol sequences, equal to the number of positions at which their symbols differ

Model A. Store on server, compare on server: PI, AD, and IR elements are all co-located on the server; during identity verification AD is passed to the PIR client as needed and the resulting PI is passed back to the server for comparison (PIC) and decision.

Model B. Store on token, compare on server: similar to Model A but with the PI, AD and IR data relocated from the server to a user-token. During verification, the client obtains AD from the token and passes the resulting PI to the server – which is responsible only for PIC and final decision.

Model C. Store on server, compare on client: similar to Model A but with the PIC and decision subsystems relocated to the client, relegating the server to the role of a pure data repository for PI, AD and IR.

Model D. Store on client, compare on client: data storage and PIC / decision subsystems are both incorporated onto the client, removing altogether the need for communication with a remote server. This might be a desirable model where suitably secure network infrastructure is not available.

Model E. Store on token, compare on client: like Model D, but divesting the PI, AD, and IR storage to a user-token.

Model F. Store on token, compare on token: this model is formally similar to Model A but with each user's PI, AD and IR data migrated from a central server to their own token, along with a suitable PIC and decision subsystem. This type of *On-Card biometric comparison* is sufficiently distinct to warrant its own ISO standard [ISO10].

Model G. Store distributed on token and server, compare on server: this model is essentially a hybrid of Models Model A and Model B, whereby the PI is retained on a centralized server but the AD and IR elements are divested to the token; a CI is introduced in order to bind the data elements across server and token. For those RBR implementations where the PI is purely cryptographic, this provides the clearest separation of PII and non-PII data. While providing a similar level of privacy protection as Models (Model D, Model E, Model F) it offers an advantage in terms of tamper resistance (which would require access to both token and server), as well as retaining the ability to revoke the credential on the server side via its PI.

Model H. Store distributed on token and client, compare on client: this model has the same partitioning of credential data as Model G but dispenses with the server by moving PI, PIC and decision subsystems into the biometric capture / PIR client. In the terms of ISO 24745 this represents a *kiosk* system.

The architecture proposed in this document does not clearly fall into any of the identified ISO architectures. Our architecture most closely resembles the Model G, and Model H architectures (shown in Figure 3 and Figure 4, respectively). The main reason our model does not fall into any of the ISO prototype architectures is that we store the digitally signed PI, not on the server, not on the client, but rather on the token. There will be further discussion of this difference in Chapter 5: Evaluation and Assessment.

Figure 3. ISO 24745 "Model G" Architecture for RBR

The ISO Model G architecture for RBR verification is reproduced here. As described in [ISO11], during verification, the token publishes the AD and CI to the client. The client captures probe biometric data and transforms it to a PI*. The PI* and CI are transferred to the server. The server compares PI and PI* resulting in a verification outcome.

There are three variations of this model can be employed [ISO11]: 1) IR stored on the server instead of the token; 2) storage of CI, IR, AD on the client and PI, CI on the server without the need for a token; 3) storage of PI on both the token as well as on the server to allow three-factor authentication at the server side.

Figure 4. ISO 24745 "Model H" Architecture for RBR

In the ISO Model H architecture, the PI and CI are stored on the client. ISO 24745 proposes that this architecture is appropriate for a kiosk application. The application presented in this document differs from Model H in that no PI is stored on the kiosk.

Vulnerabilities

Taking our lead from the BioKeyS III-Final Report [Bund11], we divide the potential attack surfaces of a privacy-enhanced biometric system into two broad classes: *insertion vulnerabilities* which primarily affect the operational security of the system, and *eavesdropping vulnerabilities* which primarily affect the privacy of PII.

While providing a useful checklist for hardening a given biometric system, in practice the mechanics of any particular attack are likely to involve multiple surfaces. For example, a spoofed fingerprint might be obtained from latent images, or constructed by means of a score-based attack such as an offline FAR or hill-climbing attack. Furthermore, attacks might be mounted using only public data (which we would not consider to be eavesdropping) given sufficient knowledge of the encryption scheme.

Adler [Adl04] demonstrated a hill-climbing attack against the Biometric Encryption scheme of Soutar et al. [Sou98] (also known in the literature as the Mytec2 scheme). Scheirer and Boult [SB07] subsequently identified a number of specific attacks against the 'fuzzy' schemes of Juels et al. [JW99][JS02]. A thorough modern review of those vulnerabilities is provided by Stoianov, Kevenaar and van der Veen [Sto09], who also identify two new attacks against ECC-based fuzzy cryptosystems and an additional class of Non Randomness attacks. We outline the main results below.

Attack surfaces

Insertion vulnerabilities

Insertion in this context consists of replacing part or all of a renewable biometric reference record in such a way as to allow an attacker to gain illegitimate acceptance by the system. At a fundamental level, it includes physical attacks such as spoofing the data capture subsystem with fake biometric samples constructed from sources such as latent fingerprints or surreptitiously obtained biometric template data; replaying or tampering with the raw biometric or extracted feature template of either the verification presentation or stored data at a point before the comparison subsystem; and substituting the stored biometric reference with one of the attacker's choosing. All of these can be mitigated by operational level security arrangements, either through technological measures such as tamper proofing and ensuring presentation liveness [NIST11], or by the use of supervising personnel to limit physical access to the system components.

Eavesdropping vulnerabilities

Eavesdropping in this context consists in obtaining illegitimately some or all of a biometric record, either for the purpose of mounting a subsequent attack on the system (or on another biometric system), or for other illicit uses such as identity theft. As with insertion vulnerabilities, these can occur either at the raw biometric level such as pulling latent fingerprints from an input device, or at the template level by

intercepting or extracting the feature data. Again mitigation can be implemented in the high level system design - for example by using rasterized fingerprint scanners rather than platten-based devices to avoid persistence of latent prints, as well as ensuring good physical security.

It should be noted at this point that the privacy-enhanced biometrics that we are considering in this report are inherently resistant to certain types of eavesdropping vulnerabilities, since they neither store nor compare either the raw biometric or extracted biometric feature set (template). Instead, they use cryptographically strong one-way functions to generate a reference that is biometrically-derived but not in itself biometric. A full information-theoretic analysis of the extent to which such functions are able to hide an individual's PII is beyond the scope of this document, and the interested reader is referred to [Bis13][DRS04]. In such schemes, biometric PII is only present transiently and is not retained within the system. Stoianov [Sto10] discusses this aspect of privacy-enhanced biometrics in more detail from the point of view of homomorphic cryptosystems.

Attacks on specific privacy enhancing biometric schemes

Attacks via Record Multiplicity (ARM)

Scheirer and Boult [SB07] note that in schemes like the FCS, the random key comprises a one-time pad protecting the biometric feature vector. However the inherent symmetry allows an equivalent view in which the biometric is a one-time pad protecting the key. If the same biometric is used for multiple enrolments, this pad ceases to be a one-time use and hence there exists a possibility to correlate data between the enrolments and to recover information about the pad itself (the biometric data). Similar correlation attacks may be conceived against the FVS, where comparison of multiple records may allow the attacker to distinguish between real data points and the pseudorandom 'chaff points' that this scheme uses to obscure the user's biometric.

> **Ex.** In a scenario such as e-cash or a b-TA, a user will go to an issuer multiple times to obtain a privilege. Each of these issuance transactions corresponds to an enrolment, the multiplicity of which might be used to mount the attack. Focusing on b-TA, then, let's say each 3 years, the traveller needs to obtain a new b-TA from the issuing country over 30 years, 10 enrolment transactions would have been accumulated. If these transactions could be examined together to reverse engineer the biometric or gain ability to spoof the system, we would be susceptible to an attack via record multiplicity.

Surreptitious Key-Inversion Attack (SKI)

In the normal operation of an RBR scheme, a secret key might be obtained from the user's biometric presentation using public helper data, and its hash compared against the stored hash of the secret. In the

case of a simple verification / identification scheme, only the success or failure of the hash comparison need be revealed. In some cases the recovered secret is to be used as a conventional cryptographic key in order to access additional private data. In such cases (or when the key is obtained by tampering or eavesdropping ahead of the hash function) it may be trivial to combine the key with the public helper data in order to reveal information about the biometric input.

> **Ex.** A fuzzy commitment scheme conceals a secret c (which is chosen from a space of Hamming codewords C) using a conventional cryptographic hash h(c). During enrolment, a public helper string δ is derived from the user's biometric feature vector x by means of a code offset construction i.e. x=c+δ. During verification, a candidate codeword c' is generated from (possibly corrupted) biometric feature vector x' using δ. The original secret c is recovered from c' provided it is within the code's correctible distance, and the user's identity is confirmed if h(c')=h(c). If only the binary accept/reject decision is output from the verification process, the system is secure: however if c'=c is also revealed (perhaps by using it as a conventional cryptographic key for an encrypted file store), then it is trivial[7] to use x=c+δ to recover the biometric feature vector x from the public data δ.

Blended Substitution Attack (BSI)

A blended substitution attack is a type of insertion attack in which the attacker's own biometric data is incorporated into a user's record. For example, considering the fuzzy vault implementation, chaff points could be replaced by the elements from the attacker's biometric feature set. Scheirer and Boult [SB07] describe this kind of blending as insidious - in the sense that from the legitimate user's point of view, the inserted data would be hard to distinguish from true chaff (and hence would not be apparent as a denial of service) but would allow the attacker to gain access as well.

> **Ex**. A fuzzy vault scheme uses centralized generation and/or storage of the enrolled credentials, which are evaluations of a BCH polynomial at points determined by elements of the user's biometric feature set, plus obscuring 'chaff points'. A malicious insider (or malicious software) is able to intercept the generation and/or storage of the credential and replace some or all of the chaff points with points from another genuine FVS credential. This subsequently allows the malicious user (or her surrogate) to validate against the stored credential.

---

[7] For *binary* Hamming codes, recovery of *x* is as simple as XORing *c* with δ.

Score-based attacks

A FAR-based is a brute force attack, consisting of exploiting the probabilistic nature of the biometric match process, by which a fraction of non-genuine biometric presentations will be incorrectly identified as genuine. This behavior is characterized by a False Match Rate (FMR) or False Accept Rate (FAR). Viewed as a classification problem, there is a corresponding False Non-Match Rate (FNMR) or False Reject Rate (FRR) and the balance between FAR and FRR will depend on the chosen decision boundary. A parameterized version of the FAR-FRR boundary is often presented as a Decision Error Tradeoff (DET) curve. A suitable operating point is chosen based on the requirements of the IdMS as a whole e.g. lower FAR favours security while lower FRR increases convenience. An *online* FAR-based attack can be mitigated at the system level by techniques such as locking the system after a number of failed attempts, or artificially slowing the allowed rate of authorization attempts, however an *offline* score-based attack would have no such restriction.

Adler [Adl04] has demonstrated a hill-climbing attack against the Biometric Encryption scheme of Soutar et al. [Sou98] where such score data is available. Despite starting from an initial image that was intentionally chosen to be markedly different from the enrolled image, the template recreation algorithm was quickly able to attain a perfect match score, even though the resulting images were not very similar to the enrolled image. Stoianov, Kevenaar and van der Veen [Sto09] proposed a more efficient attack based on *partial scores*, in the case that the available helper data is structured into 'chunks' as would be the case for RS (Reed Solomon) and RM (Reed Muller) codes for example. They demonstrated their attack against the Mytec2 BE scheme and against a variety of BCH (Bose-Chaudhuri-Hocquenghem) fuzzy commitment schemes, making recommendations for suitable BCH code lengths and a novel suggestion to consider LDPC codes for the application.

Attacks using ECC output statistics

Stoianov, Kevenaar and van der Veen [Sto09] note that the error correcting codes (ECCs) currently considered for BE were optimized for communication and may not be ideal from the point of view of security. In particular they point out that while a BE ECC might be implemented with conventional hard-decoding, an adversary might make use of more sophisticated soft-decoding algorithms or erasure decodings to 'correct' beyond the assumed code bound (hence increasing the FAR). They illustrate these techniques with attacks on the schemes of Davida [DFM98] and Kanade [Kan08]. They then present a probabilistic attack in which likely codewords can be inferred chunk-by-chunk from the histograms of decoded codeword frequency against a fairly small set of probe data, with sufficient accuracy that the scheme's outer ECC is able to correct the remaining errors.

Non-randomness attacks

As reported in [SB07], Chang et al. [Cha06] considered vulnerability of the fuzzy vault scheme to an attack based on non-randomness of the chaff points. Stoianov, Kevenaar and van der Veen [Sto09] extend this class of vulnerabilities to include non-randomness of the generating biometric. In particular they assert that minimum biometric entropy is not in itself sufficient to provide security, given certain structures in the public helper data. The illustrate this assertion by demonstrating clustering in the Mytec2 BE scheme, and describing how an iris-based fuzzy commitment scheme may be vulnerable for certain choices of ECC block size (n,k). They discuss methods for randomizing the feature data, including a generalization that leads to the BioHASH scheme of [Bund11].

Detection error performance

Since the purpose of a 'fuzzy' extractor is to reliably extract a reference string from a noisy biometric input, it clearly has a potential to modify the detection error performance of the underlying biometric system. For example in the case of fuzzy extractors based on error-correcting codes (ECC), the classification performance is determined by the error correction performance of the chosen code. Ideally such an extractor would decrease the false reject rate (FRR) without any increase in false accept rate.

The BioKeyS III-Final Report [Bund11] presents classification performance results for the proposed BioHASH scheme (based on the FCS of Juels, using a Hamming distance classifier), and for a "privacy bootstrapped" scheme in which a vendor-private classifier is wrapped within a privacy-enhanced BioHASH container (Figure 5) – thus benefitting from reduced FAR of the inner classifier while retaining the enhanced security and reliable key regeneration (reduced FRR) of the FCS. They show up to an order of magnitude reduction in FAR at an FRR of 0.01% for the bootstrapped scheme.
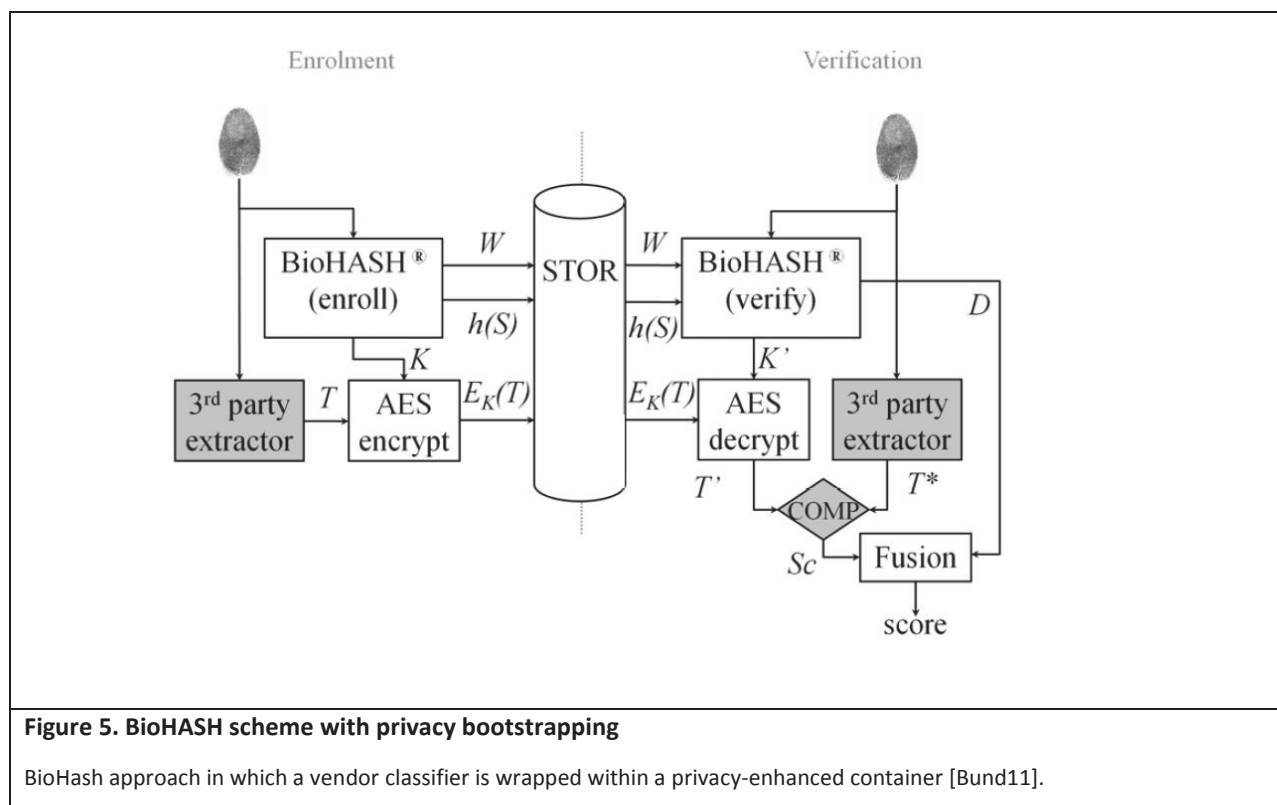
Figure 5. BioHASH scheme with privacy bootstrapping

BioHash approach in which a vendor classifier is wrapped within a privacy-enhanced container [Bund11].

Security Requirements Checklist

We present a list of requirements for the system, the user, the b-TA and the smartphone from different perspectives (including physical security and tamper resistance, false accept rate, revocability and renewability, unlinkability, non-transferability, verifiability of issuance, effective data based expiration of b-TAs, Biometric irreversibility, anonymity and selective show of attributes). For each perspective, we list a requirement (or requirements), present an example, and indicate whether each of the requirements is mandatory or optional.

Req:[1.X]   **Physical security and tamper resistance**

Req:[1.1]   **No data insertion and/or eavesdropping**

The system shall provide, or support the use of, suitable security mechanisms to prevent unauthorized data insertion and eavesdropping.

Necessity: **[Mandatory]**

Req:[1.2]   **No-leakage of intermediary outputs**

The system shall not permit access to the intermediate inputs or outputs of the biometric FE or PIC subsystems.

Necessity: **[Mandatory]**

Req:[1.3]   **No allowable blending or substitution attacks**
The system shall not permit substitution or blending by an attacker or malicious insider of either the record data or any obscuring elements such as codewords, hashes, or chaff.

Necessity: **[Mandatory]**

Req:[1.4]   **No leakage of raw biometric and extracted feature set**

The system shall not store, transmit or emit either the raw biometric or extracted feature set (template).

Necessity: **[Mandatory]**

Req:[1.5]   **No inversion of the biometrics**

The system shall not output a biometric match score in such a way as to permit any attacks, such as hill-climbing attack.

Necessity: **[Mandatory]**

Req:[1.6]   **No inversion of keys for auxiliary data**

If, in addition to providing a simple binary accept/reject record comparison decision, the system outputs a key or keys that are to be used to unlock additional cryptographically secured data, the system shall not permit the inversion of such keys, with or without the use of other available data (PI, AD) in such a way as to reveal PII.

Necessity: **[Mandatory]**

Req:[1.7]   **Appropriate Liveness detection**

If the system is to be operated without the direct oversight of authorized personnel (such as in a kiosk deployment), it shall incorporate mechanisms to mitigate biometric spoofing, such as some forms of liveness detection.

Necessity: **[Mandatory]**

Req:[2.X]　　　**Configuration of Operating Parameters**

Req:[2.1]　**Operating characteristics configurable to operational needs**
The system shall provide ability to configure operation to reach FAR and FRR that are suitable to the operational needs.

Necessity: **[Mandatory]**

Req:[3.X]　　　**Revocability and Renewability**

Req:[3.1]　**System should provide ability to revoke or cancel the credential**

In the event of a partial compromise of the IdMS (or for other operational reasons such as automatic expiry) the system shall provide the ability to revoke or cancel the credential(s) of a user.

Necessity: **[Mandatory]**

Req:[3.2]　**System should provide ability to renew the biometric reference**

In the event of a partial compromise of the IdMS (or for other operational reasons such as automatic expiry) the system shall provide the ability to create a new, distinct, credential that is based on the same biometric or combination of biometrics without increasing privacy leakage, FAR, or FRR.

Necessity: **[Mandatory]**

Req:[4.X]　　　**Unlinkability/Non-distinguishability**

Req:[4.1]　**No cross-database linkage**

It should not be possible[8] for the presence or absence of an individual's credential within any other biometric IdMS to be inferred from their credential within this IdMS.

Necessity: **[Mandatory]**

Req:[4.2]　**No record multiplicity attacks**

It should not be possible to mount an attack on the security of the system using record multiplicity from multiple enrolments of the same credential holder, either within the same system or across multiple biometric IdMS.

Necessity: *(Optional)*

Req:[5.X]　　　**Non-Transferability**

Req:[5.1]　**No b-TA lending between individuals**

It must be impossible for a b-TA issued to one individual to be used by another individual.

---

[8] The requirements "impossible" or "not possible" may be satisfied in practice by provable security under computational hard number-theoretic problems.

Necessity: **[Mandatory]**

Req:[6.X]   **Verifiability of Issuance**

Req:[6.1]   **The system must allow verification of issuer authenticity**

It should always be possible to verify the validity of the b-TA in that it was really issued by the issuer whom it is claimed issued it. Authenticity of the b-TA would not be verifiable if this were not achievable.

Necessity: **[Mandatory]**

Req:[7.X]   **Effective data based expiration of b-TAs**

Req:[7.1]   Issued b-TAs should have an expiration date after which they can no longer be used

Necessity: **[Mandatory]**

Req:[8.X]   **Biometric Irreversibility**

Req:[8.1]   If biometrics are used, it should be impossible to reverse engineer the biometric, given the data exchanged or stored at any point during the process.

Necessity: **[Mandatory]**

Req:[9.X]   **Anonymity**

Req:[9.1]   It is not necessary that application and passage transactions be anonymous.

Necessity: *(Optional)*

Req:[10.X]   **Selective show of attributes**

Req:[10.1]   It is desirable for the traveller to be able to selectively show (or retain) attributes used in the b-TA.

Necessity: *(Optional)*

Chapter 4: Selected Approach

Selected Approach

In this Chapter, we outline a possible approach for implementing an RBR solution to the b-TA scenario. In this chapter, we describe the main entities involved in the scenario, the traveller flows, and significant algorithms from a security and privacy perspective. We also describe certain special features of the algorithm including the ability to help detect passport fraud prior to boarding (optional)[9], triangular binding of b-TA to fingerprint RBR, and e-Passport, scalability to a paperless "m-Passport" application, as well as the possibility for the e-passport to be optional after the first verification.
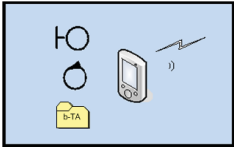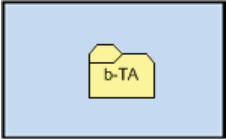
High Level Architecture

This section presents the system architecture for the proposed system. We describe the entities that participate in our proposed solution including their required knowledge as well as their behaviours and interactions.

---
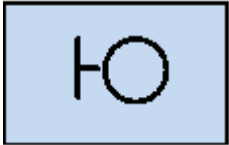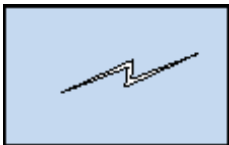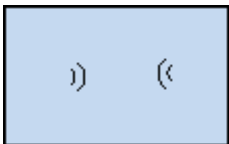
[9] Our approach features pre-departure verification of issued b-TA and optional biometric checks. These can be used to help prevent document fraud as recently occurred in Air Malaysia incident [Stastna2014] and add knowledge of travellers approaching the border before they arrive.

Figure 6. Overview of the Architecture for the proposed system

The traveller and the smartphone interact with the issuer the airline and the border authority to obtain and show ownership of the biometrically enabled b-TA.
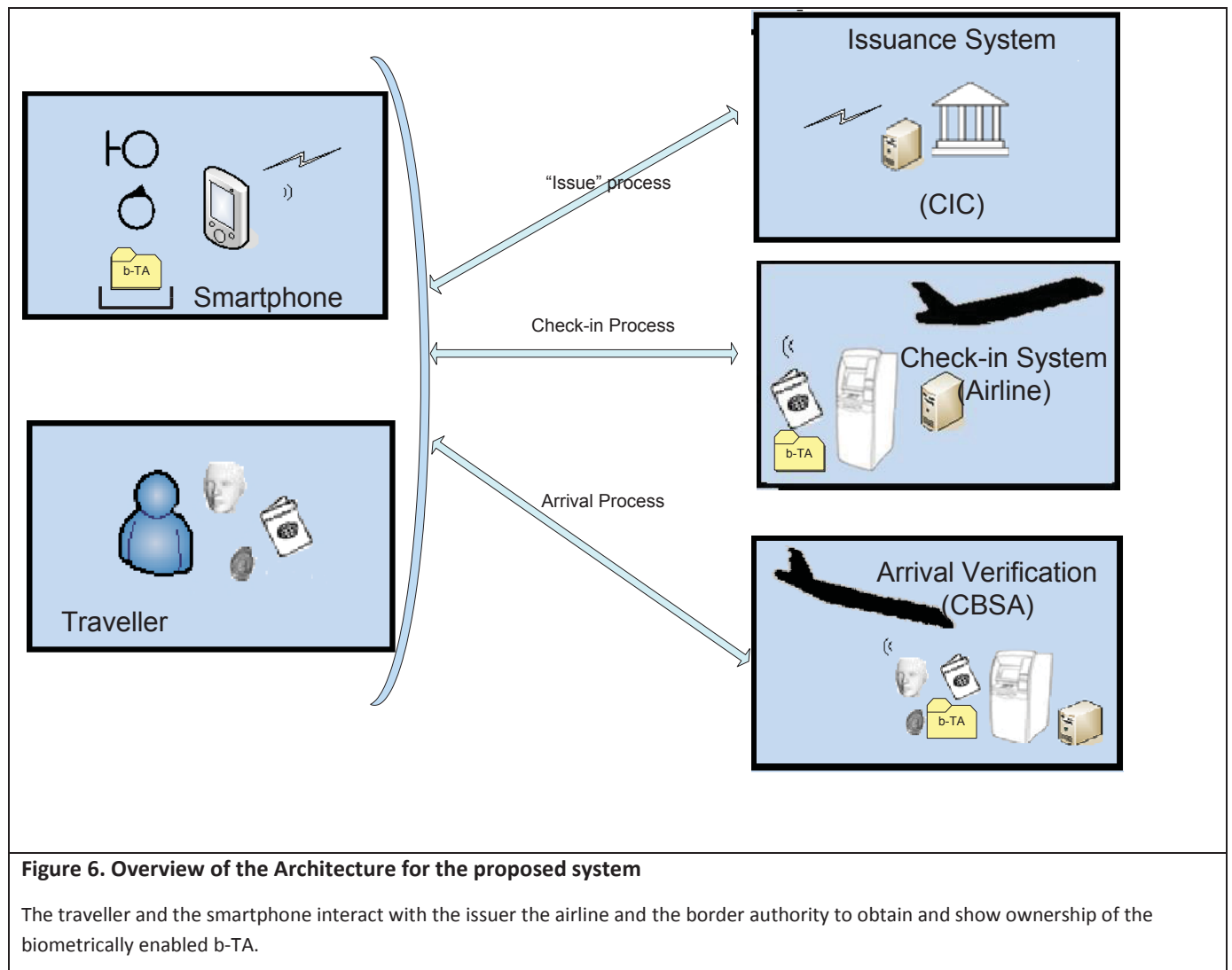
The entities in Figure 6 are described below:

	The Traveller The traveller is an individual, who holds an e-passport of a foreign country, and wishes to travel to Canada. For the proposed protocol, the traveller has an e-passport, face and fingerprint biometrics, a smart-phone with appropriate end-user application installed.
	The e-Passport The e-passport is an ICAO-compliant travel document issued by the traveller's home country. The e-passport includes a chip which can be read by the check-in and verification kiosks. The chip holds biographical information as well as a facial image of suitable quality for passport-face biometric comparison.
	The Smartphone The traveller's smartphone has the following components: 1) The b-TA (on secure storage once issued) 2) The end-user application 3) A fingerprint biometric sensor 4) Internet data communications (for the issue protocol) 5) Close proximity wireless data communication (such as Bluetooth, or near-field communication (NFC) to interface with the kiosks for ticketing and biometric verification) Each of these functions is further described below.
	The b-TA The b-TA is a digital credential issued by the country of destination to the traveller. The b-TA binds biographical, biometric, and travel authorizations (such as name, passport number, fingerprint RBR, and expiration date for the b-TA) into an electronic package signed by the issuing authority, and verifiable by the border security agency upon entry to the destination country.
	The end-user application The end-user application is a third party application which resides on the traveller's smartphone. The end-user application has the following responsibilities: 1) Coordinating user workflow for the processes of application submission, airport check-in and arrival at destination. 2) Ensuring security and privacy interests of end-user, the issuer, the verifier and the airline. 3) Storing user data in a confidential manner 4) Adhering to the protocols as defined For the proposed protocol, the device is assumed to implement secure protocols with interests of involved parties. These protocols are not explored in this study but may include Chaum's "wallet-database and observer" protocol or other e-wallet protocols [CP92].

	The Biometric Sensor The biometric sensor is a hardware device (an associated embedded software) which resides on the smartphone. The sensor is able to acquire a fingerprint biometric sample, extract an associated template; and for the proposed protocol, create an RBR from that template.
	Secure internet communications During the issue protocol, the traveller and the issuer communicate over the internet, through a wireless connection from the traveller's smartphone to the issuer's server applications.
	Issuer In our scenario, the issuer corresponds to the agency responsible for issuing travel authorities to foreign nationals. This agency is assumed to have both physical missions and technical interfaces operating overseas. In a Canadian context, an example of the issuer would be the CIC.
	Close-proximity communications Our approach features close-proximity communications between smartphone and kiosk in the check-in and arrival processes. Such communication does not need to go across the internet, but occurs within the airport, with the traveller standing at the target kiosk. Such communication could possibly be achieved using wi-fi, near-field communication (NFC) or bluetooth technologies.
	Verifier 1) The verifier operates a kiosk associated to primary, and secondary inspections in the country of destination. 2) The verifier is responsible for screening travellers for risk and granting access to the country. 3) For proposed protocol, the verifier is assumed to operate a series of biometric verification kiosks. 4) In a Canadian context, the verifier could be an agency such as the CBSA.
	Biometric Verification Kiosks 1) The biometric verification kiosk is installed in the country of arrival and is outfitted with the following components: 2) Biometric facial image capture camera 3) e-passport reader 4) e-passport verification software 5) Fingerprint sensor 6) Wireless communication to interface with smartphone 7) b-TA processing software.

Traveller Flows

Figure 7 captures the main system flows from a traveller's perspective. Each of these three flows, "application submission", "airport check-in" and "arrival at destination" are described in detail below.
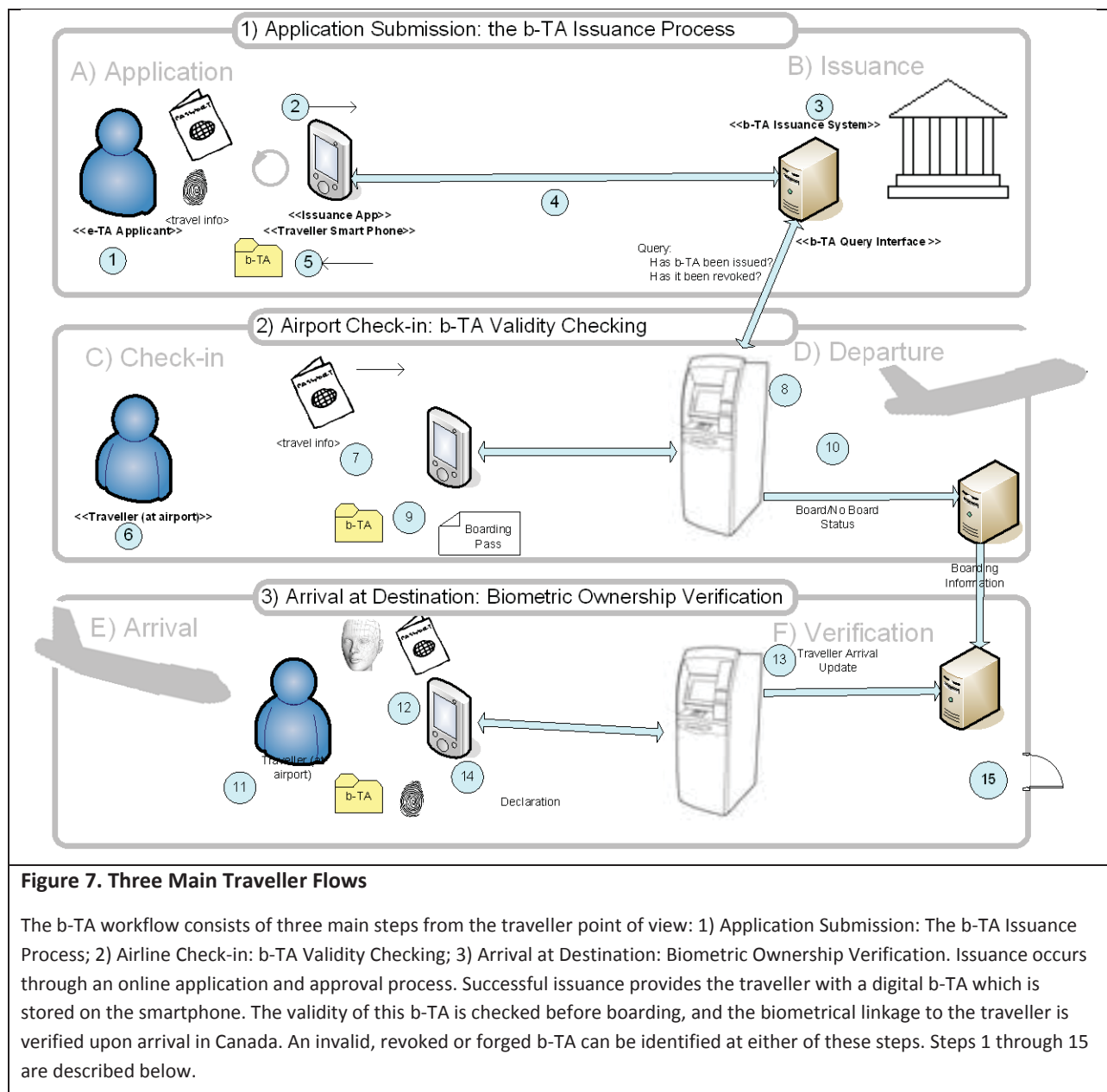
Figure 7. Three Main Traveller Flows

The b-TA workflow consists of three main steps from the traveller point of view: 1) Application Submission: The b-TA Issuance Process; 2) Airline Check-in: b-TA Validity Checking; 3) Arrival at Destination: Biometric Ownership Verification. Issuance occurs through an online application and approval process. Successful issuance provides the traveller with a digital b-TA which is stored on the smartphone. The validity of this b-TA is checked before boarding, and the biometrical linkage to the traveller is verified upon arrival in Canada. An invalid, revoked or forged b-TA can be identified at either of these steps. Steps 1 through 15 are described below.

Traveller Flow 1- Application Submission: The b-TA Issuance Process

The traveller applies online for a b-TA some time prior to departure. The traveller uses their smartphone to submit data and obtain the b-TA from the issuing organization. The entire application process is coordinated on the smartphone by a software application certified by the issuer and verifier. Once issued, the b-TA is stored on the smartphone to be used during check-in and arrival processes, until it expires.

The b-TA applicant begins the application process using a smartphone equipped with specialized software (the end-user application), a biometric sensor and secure storage capability.

1	**The traveller begins the b-TA application procedure** The end-user application coordinates user workflow including data collection, generation of an RBR, and communication with the back-end b-TA Issuing system. The end-user application maintains secure storage which is able to store user data in a reliable manner such that this information is not released to external parties.
2	**End-user application submits b-TA application** The end-user application provides the interface to facilitate submitting all required pieces for the online b-TA application procedure. This information includes biographical data, biometric data and information regarding travel intent. The biometric data consists, not of a traditional biometric template or image, but of an RBR which the smartphone generates using the traveller's fingerprint, random data, and publically available group parameters. The end-user application uses wireless communication to transfer information to the issuance server application upon request of the traveller.
3	**Issuer verifies submitted application** The issuer performs an initial check on the submitted information to see if the traveller can be granted a b-TA using the online application service. The approval process may include queries to other core systems record keeping, and manual processes. This attribute check occurs offline: the length of the process does not impact the protocol we present. Upon successful completion of the attribute verification step, the issuer sends a notification to the applicant to proceed to next step: retrieval of the granted b-TA.
4	**Retrieval of the b-TA** To retrieve the b-TA, the user agent and the issuance server application enter into a secure protocol in which the issuer signs the b-TA, and the traveller obtains this signed b-TA and any required helper data.
5	**b-TA is stored** The signed b-TA and any associated helper data are stored on the cell phone in a secure manner, to be used at a later date (i.e. at the airport to register for boarding).

Table 1 Issuance Flow

Traveller Flow 2- Airport Check-in: b-TA Validity Checking

At the departure airport, the traveller goes through the check-in procedures of the airline. These include a step in which the b-TA is verified for validity. This validity checking occurs in a wireless protocol between the end-user application on the traveller's smartphone and the airline kiosk, as well as system to system queries between the airline kiosk and the Issuer's b-TA query system. The kiosk verifies that travel is occurring within the allowed b-TA effective dates, that the b-TA has not been tampered with, and that travel privileges have not been revoked. No biometric check is performed at this stage. On successful completion of the check, the traveller can board the flight and proceed to the destination country.

6	**The traveller begins the Check-in process**
	The traveller approaches the kiosk at the airport of origin to check-in and to obtain a boarding pass. The traveller has a smartphone equipped with the b-TA application and an issued b-TA.
7	**The traveller submits required check-in information**
	The traveller enters required information at the airline check-in kiosk. This information can include name, destination, flight and b-TA number. The information can be entered automatically from the smartphone using wireless communication and using an e-passport reader. No biometric verification is performed at this stage: it occurs in the next step upon arrival in the destination country. (To note, a biometric check of fingerprint for b-TA and face for e-Passport could be added here. These would increase the cost of the check-in kiosk.)
8	**The check-in kiosk processes submitted information**
	The airline's kiosk performs a validation of the information submitted.
	This includes a verification the b-TA has indeed been correctly issued and has not been revoked. These checks can occur simply using an online query to the issuer system.
	The kiosk also verifies that the expiration date has not been reached.
	Important note: Passport fraud at boarding time can be detected by adding biometric verification to the airline kiosk. The traveller's face can be compared to the e-passport or a captured fingerprint can be compared against b-TA[10].
9	**The check-in kiosk provides next step information**
	If the check is successful, the kiosk may issue a printed token, or an electronic token and the traveler proceeds to "the next step" in the check-in and boarding process. This may be, a security or baggage processing step or the issuance of a boarding pass.
10	**The traveller proceeds to next step in departure**
	The traveller proceeds to "the next step" as deemed by the kiosk, possibly using a token dispensed by the kiosk (such as a boarding pass). The airline also maintains any departure information records as needed.

Table 2 Check-in Flow

---

[10] Biometric verification at airline check-in can help prevent passport fraud [Stastna2014]

Traveller Flow 3- Arrival at Destination: Biometric Ownership Verification

At the destination country the traveller disembarks and proceeds to the verification kiosk. The verification kiosk and the smartphone engage in a protocol to verify the user's fingerprint against the fingerprint RBR in the b-TA. For first time travel, the traveller's passport and passport biometric are also verified and cross-verified with b-TA information, as described in the "Passport may be Optional after First Verification" section.

11	**The traveller begins the arrival process**
	The traveller arrives at the destination airport. The traveller has a smartphone on which is stored the issued b-TA and supporting data. The interaction at the airport occurs with a biometric kiosk maintained by the destination country's border security agency. The kiosk will verify the authenticity of the credentials and the ownership of the b-TA through a biometric verification.
12	**The traveller provides arrival information**
	Upon arrival the traveller initiates a session with the kiosk to provide passport information, b-TA information, and required biometrics to prove ownership of these.
13	**The kiosk processes the information**
	The kiosk reads the provided e-passport information including traveler name, passport number and the enrolment facial image captured by the issuing country. The kiosk captures another facial image and a fingerprint from the traveller.
	The passport face is matched to the travellers face.
	The kiosk may also send a copy of the face image to other systems for screening purposes depending on the requirements of the international agencies involved.
14	**Passenger arrival is recorded**
	After having performed all verifications, the stored records are maintained. (As indicated in Figure 7, this can include updates to databases (see label 14a) as well as tokens issued to the user (see label 14b).
15	**Passenger continues through arrival process**
	Having cleared the verification of e-passport and b-TA, the traveller can proceed to other arrival processes.

Table 3 Verification Flow

Description of Key Algorithms

This section provides an overview of some of the algorithms relevant from a security and privacy perspective. Where an in depth description is required, the reader is referred to the primary literature.

System setup

The system set up includes configuration of algorithms and data for smartphone, issuance system, and verification kiosk. This includes configuration of mathematical parameters needed for commitment generation parameters required for the verification of the issuer's digital signature and public and private keys required for RSA-OAEP [BR94].

Key Algorithms: Traveller Flow 1 - Application
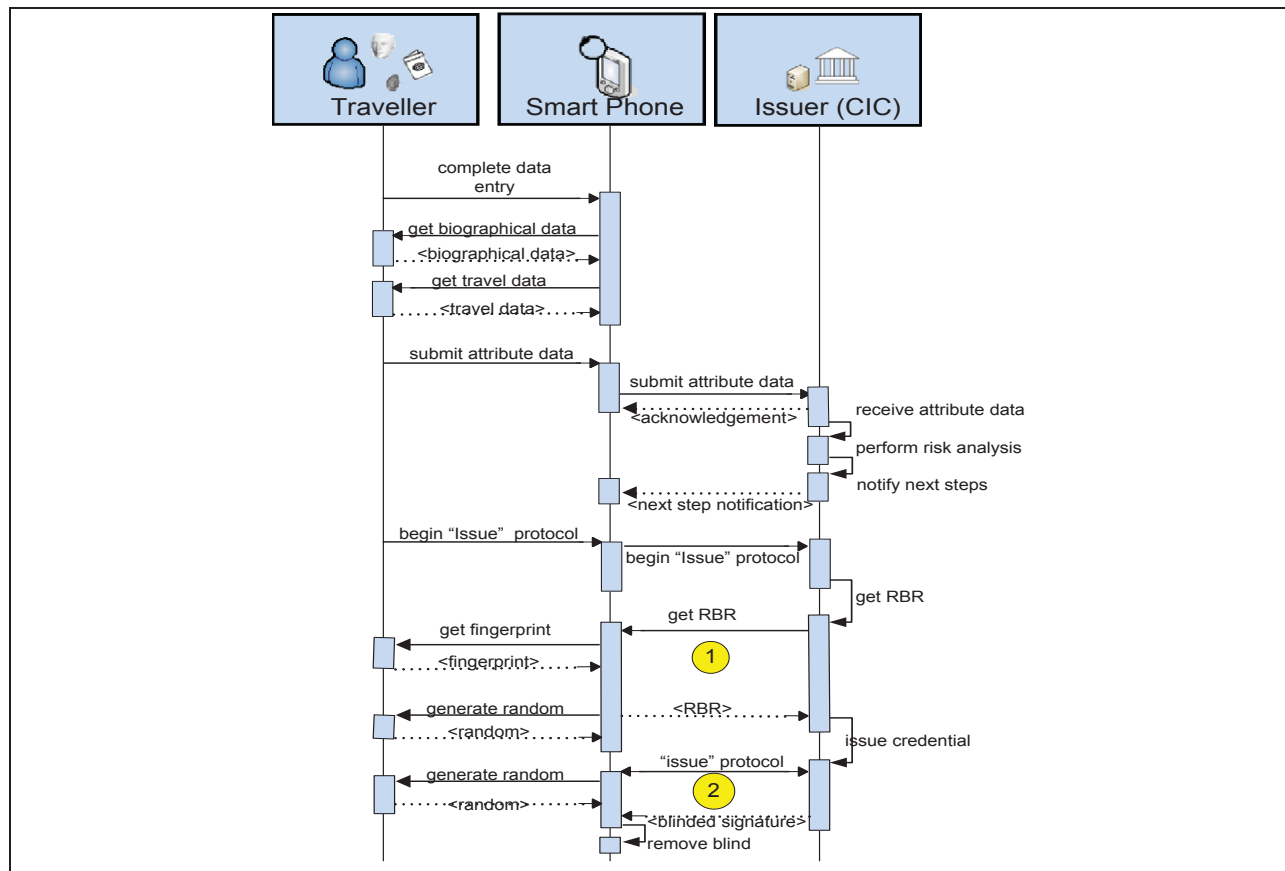
Figure 8. Important algorithms in the "Application and Issuance" step

The b-TA application and issuance step includes two algorithms with security and privacy significance: label (1) the generation of the fingerprint RBR, and label 2) the secure protocol in which the b-TA is constructed and signed

Algorithm 1: Issuance-time RBR Capture

The traveller's smartphone is responsible for capturing the imprint of the traveller's fingerprint generating the RBR which will subsequently be submitted to the issuer to be sealed into the b-TA. This can be achieved using any RBR generation mechanism. We illustrate using a variation of the scheme presented in [Bis13].
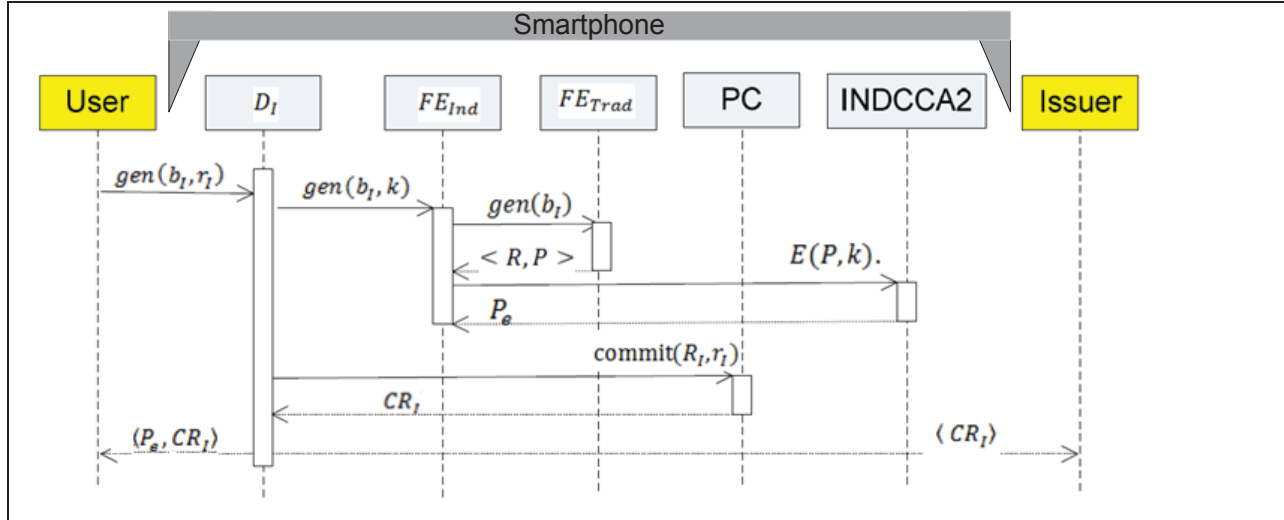
Figure 9. Generation of the Issue-time Renewable Biometric Reference.

The RBR is generated on the smartphone using the sensor and custom software embedded within it. The user supplies the biometric b_I, and accompanying random data r_I, the system provides the RBR CR_I, and accompanying public data P_e. The RBR is also provided to the issuer, who will eventually seal it into the b-TA in the cryptographic credential's *is*sue protocol.

The RBR is generated on the smartphone using the fuzzy extractor indistinguishability adapter (FE_{Ind}) configured in *issue* mode, as described in [Bis13]. We briefly describe the mechanism here, but defer the reader to the primary literature for a full description.

First, the smartphone captures the fingerprint impression and produces biometric template b_I. This template is passed to the $gen(...)$ method of the FE_{Ind} which generates the fuzzy extractor tuple $< R, P_e >$ which are obtained by encrypting the public data P obtained from the underlying fuzzy extractor with the encryption key k. The cryptographic key R obtained from the fuzzy extractor is combined with a random value r_I to produce the renewable biometric reference CR_I , a Pederson commitment [Ped92][Dam99] on those values.

The values of P_e, and CR_I are retained on the smartphone. The value of CR_I will be sent to the issuer as a RBR.

Algorithm 2: b-TA Issue Protocol

The b-TA *issue* protocol is an interactive protocol between the traveller and issuer, and is implemented using the *show* Protocol of the selected credential. We will use Brand's digital credential protocol, augmented with the biometric binding approach defined in [Bis13].

In the b-TA workflow, once the attributes and RBR have been submitted to the issuer, the actual b-TA calculated and signed using the *issue* protocol of the underlying cryptographic credential scheme. In the context of our discussion, the attributes X = $\{ x_1, \ldots, x_n \}$ have already been sent to the issuer as well as the RBR CR_I which has been set into a designated attribute x_l. Thus steps 1 and 2 of the *issue* protocol are completed. From here, the protocol proceeds as per [Bra00], the traveller and issuer collaboratively participate in the process to obtain the issuer's cryptographic signature on the RBR credential. At the end of this process, the traveller obtains the tuple $C = \langle h', (c_0', r_0') \rangle$ which consists of the credential h' and the issuer's cryptographic signature (c_0', r_0'). Together we view these as the public portion of the b-TA, which will be provided later to the verifier, who will ascertain that the data is properly signed and has not been tampered with.

Key Algorithms: Traveller Flow 2 - Departure

Figure 10. Important algorithms in the "Airport Check-in" step

The check-in procedure at the airport includes only one algorithm of importance from a security and privacy perspective. At label 3), the smart-phone and the airline kiosk must exchange an identifier to verify that the b-TA has been issued. The traveller's passport number can be used in a remote query on the issuer database.

Algorithm 3: b-TA preparation for Airline check-in

In the second traveller flow, when the traveller checks in at the departure airport, the only identified interaction having possible impact on privacy or biometric security is the exchange of information from smartphone to check-in kiosk, and the associated query on the issuers system to verify that the b-TA has been issued.

The question to be answered here is what kind of anonymity is required to the traveller's check-in transaction. As discussed in Section 2, anonymity of the traveller and unlinkability of transactions is not a requirement between Canadian agencies in the b-TA application: it is acceptable for the airline, the immigration authority, and the border agency to all know and communicate the passport number.

From that perspective, then, algorithm 3 in Figure 10 becomes straight-forward. In it's simplest form, the traveller communicates her passport number to the kiosk, which is then used to query against the

issuer database. If a b-TA has been issued on that passport number, the traveller is granted permission to proceed.

A stronger verification can be performed by sending an identifier for the b-TA to the issuer [Bis13][Bra00]. Using this approach, the smartphone sends both passport number and b-TA identifer to the kiosk, the kiosk queries the issuer's database to verify that the particular b-TA was issued to the given traveller. If the check verifies, the traveller is granted authority to proceed to the next step.

At this point, the issuer can also inform the check-in kiosk if the b-TA has been revoked.

Key Algorithms: Traveller Flow 3 - Arrival

Figure 11. Important algorithms in the "Arrival" step

The verification procedures at arrival include capturing a fresh RBR and verifying that it corresponds to the RBR which was sealed in the b-TA at the time of issuance. The issuer may perform a status update and/or record maintenance in a passage database which streamlines subsequent checks by other government agencies, as well as processing for subsequent arrivals (see "General Discussion" section). Within this process, significant algorithms from a security perspective are labelled above, where (4) represents the regeneration of the fingerprint RBR and (5) represents the verification of b-TA integrity and entry privilege.

Algorithm 4: Generation of verification-time RBR
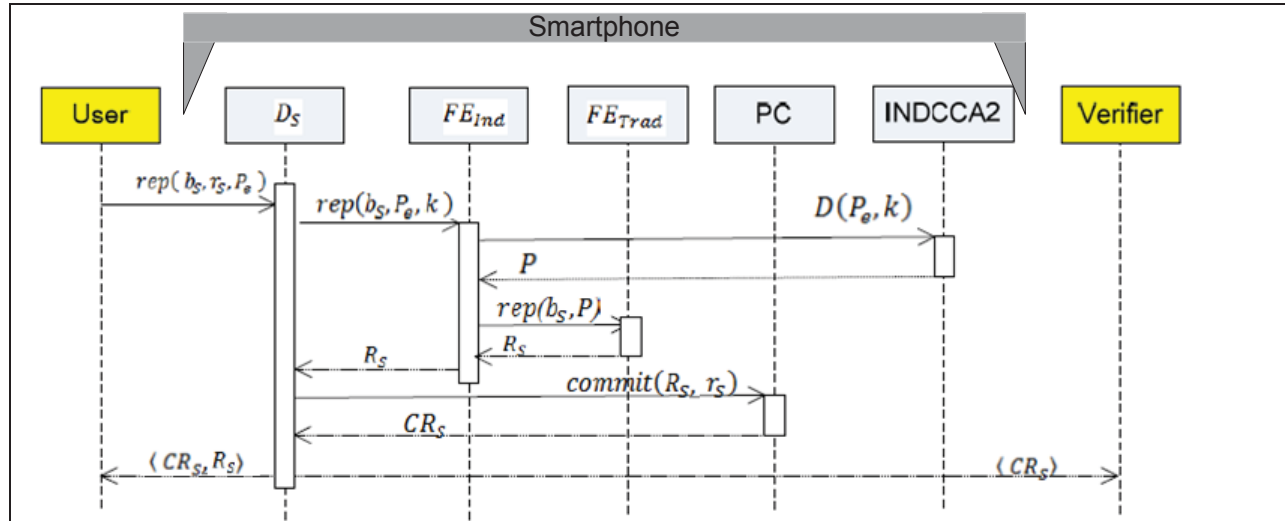
Figure 12. Generation of the verification of RBR.

Upon arrival, a fresh biometric is captured, using the kiosk. The kiosk is equipped with show time device functionality as defined in [Bis13].

On arrival at the airport of destination, the traveler's ownership of the b-TA must be established. The first step in this process is the creation CR_S: the verification-time instance of the RBR.

This algorithm creates a Pedersen Commitment on the Fuzzy Extractor R value as was done in Algorithm 1. Here, however, rather than the biometric capture and RBR generation being performed on the smartphone, it is performed on the verification kiosk.

To create CR_S, the traveller initiates communication with the kiosk which allows P_e to and r_S to be transferred. The traveller also supplies a fingerprint imprint to the kiosk. The kiosk then generates the CR_S.

First, the smartphone and the kiosk enter into communication. The user then submits a fingerprint impression and produces a biometric template b_S. This template is passed to the $rep(...)$ method of the FE_{Ind} which regenerates a biometric key R_S. This R_S is sealed in a Pedersen Commitment CR_S which then becomes the verification time RBR [Bis14].

CR_S and R_S are provided the traveler to use subsequent steps in the verification process.

Algorithm 5: *Show* Protocol

After the RBR has been regenerated by the arrival kiosk, the final step in the workflow requires verification of the b-TA, the e-Passport, ownership thereof, and the claimed travel priviledge. This requires the verifier to become convinced that:

1) the b-TA data package has not been tampered with,
2) the RBR sealed into the b-TA and regenerated in the previous step are the same biometric,
3) the e-passport number within the b-TA corresponds to that of the passport held by the traveller,
4) the traveller's face and the face image on the e-passport match, and
5) that the traveller claim of privilege is valid.

To verify that the digital package has not been tampered with, a verification relation is evaluated by the verifier. This verification relation is defined by the underlying credential scheme. In general it is a function of the credential itself, and the issuer's public key. The public key may be installed on the kiosk itself, or can be accessed through an online connection.

Once the verification relation has been checked, the traveller proves ownership of b-TA. This is done by proving that the RBR within the b-TA generated by the kiosk on arrival are derived from the biometrics of the same individual. This is achieved using a ZKPoK $DLRepWithPC$ which verified that CR_I and CR_S are commitments on the same derived key R_S. A detailed description of the protocol $DLRepWithPC$ is available in [Bis13] [Bis14] and [Ada11].

Following proof of biometric ownership of the b-TA, the smartphone and the kiosk engage in a check that the b-TA allows entry into the country, that it is within appropriate entry dates, and it has not been revoked. This can be proven using a combination of the statement proof mechanism of the underlying credential system [Bra00], and online revocation checks with the issuing authority.

Selected Discussions

This section includes some discussion of select features to note about the proposed approach. This includes a mapping of the technical components used to the ISO language previously introduced, a description of possible contents of the b-TA, a discussion of the triangular binding and a discussion of the ability of this approach to scale to multiple nations and paperless passports.

Mapping to ISO Terms

The technical constructs used in our approach can be mapped to the terms used by the ISO (as discussed in Chapter 3). For convenience, Figure 13 reproduces the ISO model for RBRs in an Enrolment and Verification environment. It should be noted that the ISO diagram below models an architecture in which the PI is stored in the database, and transferred to the comparator at verification time. In our architecture the PI is stored on the token, and transferred from the token to the comparator at verification time.

Figure 13. ISO Architecture for Renewable Biometric References

ISO architecture for enrolment and verification with RBRs which shows creation and regeneration as well as comparison of RBR.
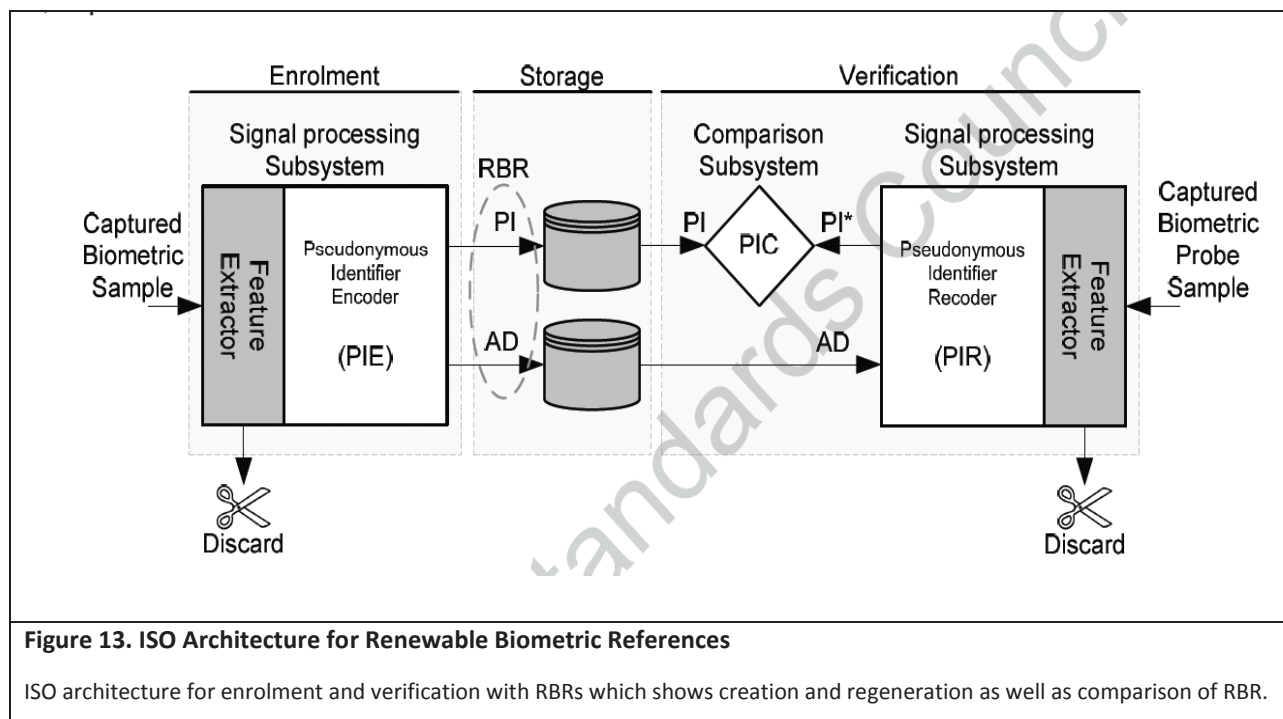
The mapping of the terminology used in our approach to that of the ISO is shown in Table 4.

Table 4 Terminology Mapping to ISO Model

Acronym	Expansion	Equivalent in Proposed Architecture
PIE	Pseudonymous Identifier Encoder	The *gen(…)* method of the Fuzzy Extractor
PIR	Pseudonymous Identifier Recorder	The *rep(…)* method of the Fuzzy Extractor
PIC	Pseudonymous Identifier Comparator	*DLRepWithPC*
RBR:	Renewable Biometric Reference	
PI	Pseudonymous Identifier	CR_I , R_I
PI*	Candidate Pseudonymous Identifier	CR_S, R_S
AD	Auxiliary Data	P, P_e

Our model is a hybrid between Models G and H:

1) In Model G, PI and CI are stored on a server, and comparison at verification time occurs at the server
2) In Model H, PI and CI are stored on the kiosk, and comparison at the time of verification occurs on the kiosk

Table 5 summarizes the key features of the ISO Model G and H architectures and illustrates how our approach combines features of each.

Table 5 Summary of Architectural Differences

Approach	Storage of PI, CI	Verification Comparison
ISO Model G	Token	Server
ISO Model H	Client	Kiosk
Our Approach	Token	Kiosk

Our application maps to the ISO architecture as shown in Figure 14. The numbered flows show:

1) the sensor on the smartphone gathering the biometric, and sequencing generation of the PI through the augmented fuzzy extractor mechanism
2) The attribute data being sent to the issuer (which including the PI)
3) The credential and accompanying signature being returned to the smartphone for storage and future use
4) Verification of credential integrity by the verifier
5) Reproduction of PI by the PIR which is resident on the verifier's kiosk
6) PIC preforming comparison using ZKPoK (DLRepWithPC)
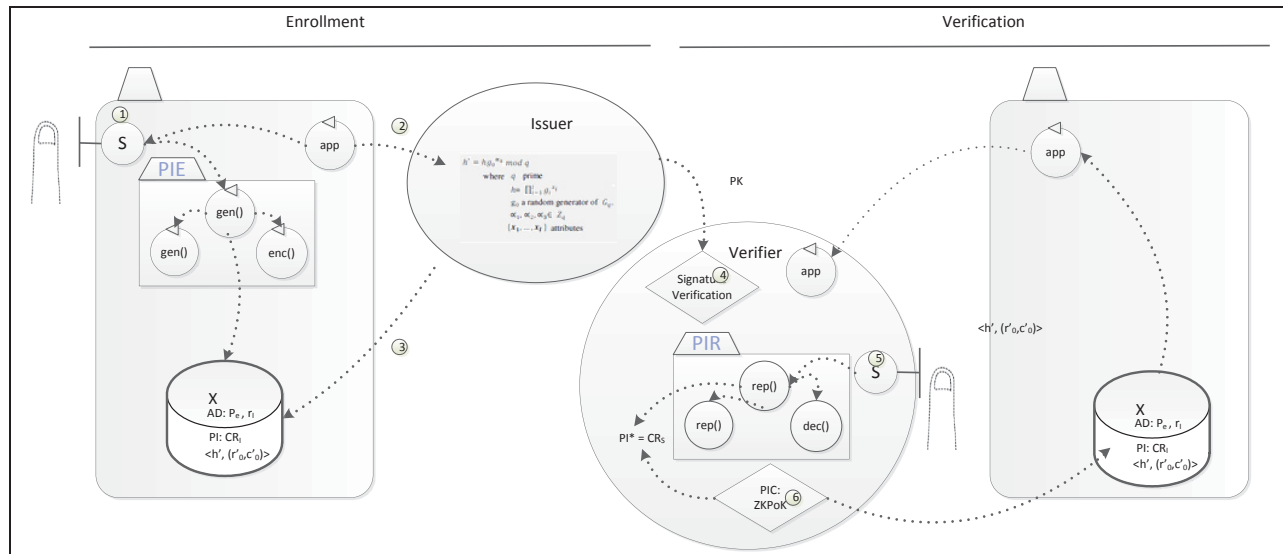
Figure 14. Proposed Architecture in ISO Terms

The proposed architecture can be expressed in terms of the ISO architecture to highlight some interesting features.

Some items to note include:

1) The biometric is not saved by either sensor
2) By design we include a certain asymmetry: PI generation occurs on the smartphone while PI* is generated by the kiosk.
3) The PI generated at enrolment time never leaves the cellphone
4) Our design is analogous to a biometric-on-card design. No cross-system call is required at verification time to retrieve PI. Rather, the Original PI is accessed (indirectly) from the cellphone. A cross-system call is needed to access the issuer's digital signature public key.
5) The AD is stored on the smartphone (not provided to the Issuer). The AD is provided to the Verifier to reconstruct PI*
6) Our proposal's architecture is not analogous to either ISO Model G or Model H:
   "In contrast to model G, our proposed architecture does not store PI on the server. As a result, we provide higher scalability in an international time since no calls from verifier system to issuer system are required to retrieve traveller PI."
   "In contrast to model H, our proposed system does not store PI on the kiosk. This would be impractical in an travel system potentially open to all travellers of participating nations"

e-Travel Authority Sample Contents

The b-TA is a large numeric value. It can be thought of as a digital digest of multiple traveller attributes, signed by the issuing agency. The digest can contain any number of attributes of the traveller.
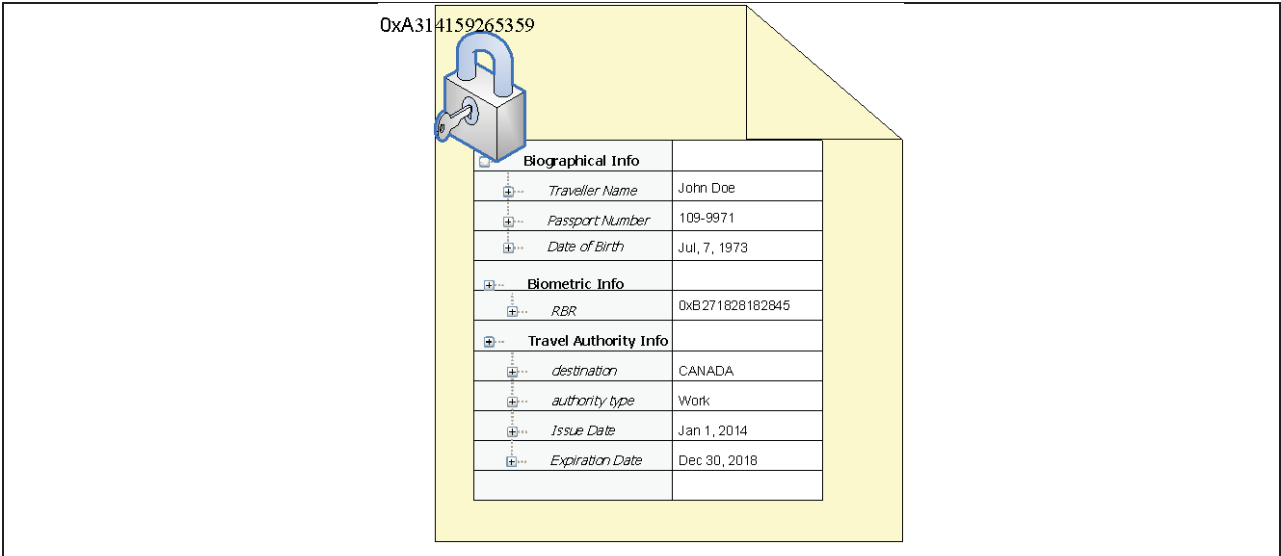
Figure 15. Sample of the contents inside a b-TA

The b-TA itself is a numeric digest that is composed of traveller attributes which include the fingerprint RBR. The items includes within the b-TA will be decided by the issuing and verifying authorities but may include biographical, biometric and travel intent/permission information. In the issuance process the b-TA is digitally signed by the issuer so that its contents become tamper-proof.

Figure 15 represents a diagram of the b-TA as a numeric value which binds a collection of data. In the above example, we illustrate three important categories of information: Biographical information, Biometric information, and travel authority information. We provide sample values to illustrate the type of information each item could hold.

The biographical information can include traveller's name, passport number, date of birth and other civil registry information. Inclusion of the passport number allows the issued b-TA to be linked to the e-Passport, which is important for the initial verification of identity. In terms of digital credentials, each of these attributes is transformed into a number, given a position in the vector of attributes, exchanged with the issuer and signed into the credential through the *issue* protocol.

To highlight the point that the RBR, and the digital credential are simply large decimal numbers (and not more complex data structure such as a collection of key-value pairs), Figure 15 gives arbitrary values to the b-TA and the RBR (0xA314159265359 and 0xB271828182845, respectively). While specific

attribute values are provided in the application, once the issue process is completed the public part of the b-TA corresponds to a large numeric value.

At the time of verification, the kiosk verifies an assertion about the sealed attributes in the b-TA. An example of such an assertion could be, "the traveller's passport number is 109-9971, the traveller is authorized to enter Canada, and the traveller's RBR is 0xB271828182845 and this information is valid until Dec 30, 2018.

Triangular Biometric Bindings

Figure 16 illustrates how the b-TA binds to the traveller's RBR, and the traveller's e-passport. These relations enable security to be linked to an identity, and offer the potential for the b-TA to replace the e-passport after the initial verification (see: "Passport may be Optional after First Verification " below) .
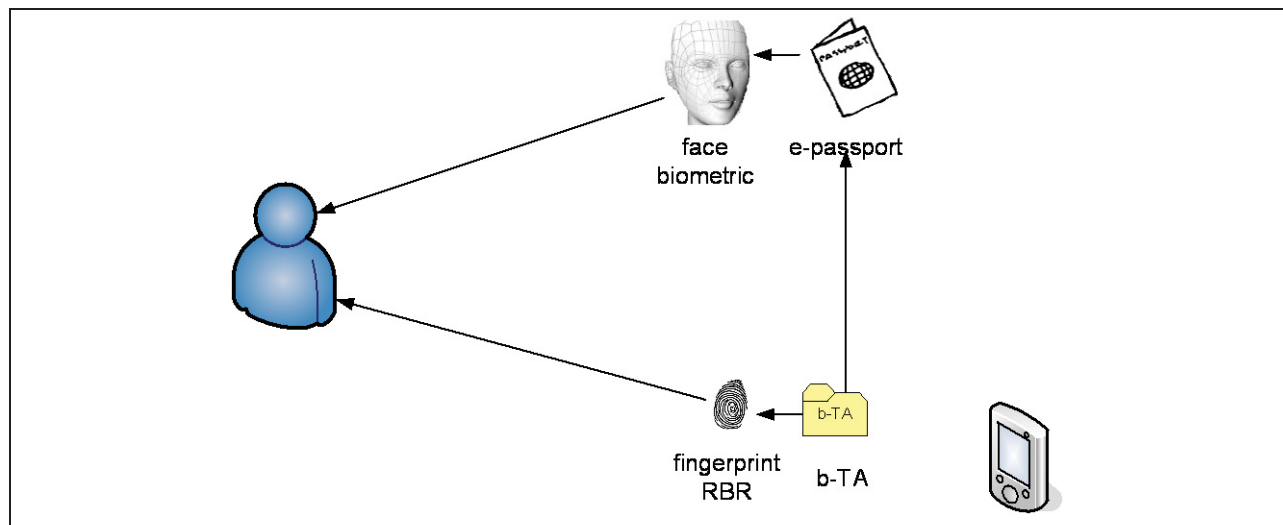
Figure 16. Triangular bindings between issued documents.

The b-TA is bound to the e-passport number as well as the traveller's fingerprint RBR in a tamper-proof manner. This results in two biometric linkages which provide strength of security but also enables operational efficiency and traveller convenience in terms of streamlining second passages and online application.

The kiosk at arrival is responsible for both facial recognition and fingerprint RBR verification.

The e-travel authority is cryptographically bound to the passport number as well as the traveller's RBR. The traveller's identity is thus bound to both the e-passport and the b-TA. The b-TA is bound to the passport number and to a RBR created using the traveller's fingerprint. The traveller's identity is bound to both the e-passport and the b-TA. The e-passport binding occurs through the issuing country's adherence to ICAO e-passport standards. While these standards are indeed quite high, and demanding, there is a certain variability in the processes and documents issued within the international community. The

Canadian Government has no control on the processes followed by individual issuers. The b-TA is bound per agreement between the issuer and the verifier. In the context of this report, these are both Canadian Agencies.

Four important lifecycle steps in identity binding and verification are required:

Step 0) The e-passport is issued

Before anything occurs in the b-TA steps, the passport must be issued. The foreign country issues an e-passport to the individual, a foreign national. At the point of e-passport issuance, any number of procedures is followed including background checks and updates to the civil registry. Different countries will have different processes. The e-passport is produced in accord to ICAO e-passport standards and includes an electronic file with the individual's passport image.

Step 1) The b-TA is issued

The applicant's submits informational attributes (which include at least an e-passport number and RBR) to the issuing organization. The issuer performs a background check, and issues the b-TA. The b-TA is bound to the attributes in a manner which prevents the attributes from being changed without invalidating the digital signature. At this point, the traveller's identity and ownership of biometric is assumed, but has not yet been verified.

Step 2) First arrival:

The first time the traveller arrives to visit the country that issued the b-TA, the biometric linkage between b-TA has not yet been verified. On first arrival, the kiosk verifies the e-Passport biometric, the b-TA biometric and the passport number contained in the b-TA. On successful verification, the verifier may record the passage in a database, and issue a "verified entry" credential to be retained by the traveller to simplify further processing, on this trip and on subsequent trips.

Step 3) Subsequent arrivals:

After successful verification on the first arrival, the processing of subsequent arrivals may be stream-lined. If the verifier chooses to issue "verified entry" credentials for first arrival, this can be checked on subsequent arrivals potentially making the e-passport verification optional.

m-Passports: An electronic wallet approach for b-TA

What about the scenario where a traveller holds b-TAs for multiple countries?

We have presented an application which manages the workflow necessary to obtain, view, modify and use a Canadian b-TA. It can be extended to a multi-nation scenario. While beyond the scope of this study to do so, we provide a sketch to highlight the potential. We name this functionality m-Passport, to mean a mobile paper-less passport, stored on a cellphone.

We may consider the scenario where multiple nations each issue their own b-TA to travelers and the traveller thus has a collection of b-TAs to manage. This leads to a more sophisticated user agent application which allows the traveller to store many such b-TAs: we highlight this possibility and refer to it generically as an m-Passport, or an electronic wallet. This m-Passport would be analogous to a passport in that it would be certified as belonging to the given traveller, issued by the country of citizenship, and a cumulative record of travel authorities and travel passages.

In order to make this, the following are required:
1) A more sophisticated user application is required,
2) A smartphone construct allowing secure and selective read and write permissions
3) A cryptographic credential corresponding to an electronic citizenship card
4) Selective show and an ability to show across credentials issued by multiple issuers.
5) Standards within and across Issuer and Verifier communities

Currently, as internet commerce reaches high levels of technical maturity, there are a number of market offerings which may lend themselves to this kind of applications, including Microsoft's UProve, or IBM's Idemix, which implement the base credential schemes described in this document. Within the literature, one can refer to Chaum and Pedersen's 1992 paper, "Wallet Databases with Observers" [CP92] which sets foundations for secure wallets.

While this should be the subject of future study, there is no evident requirement for all countries to use the same attributes for the issuance and verification of b-TAs. It seems that the responsibility for the definition of these fields may be left with the issuance and verification bodies of each nation.

National certificates of identity, on the other hand, correspond to the personal identification block on a traditional e-Passport. As these will need to be read by multiple nations, it seems standardization will be required. These standards may follow [ICAO9303].
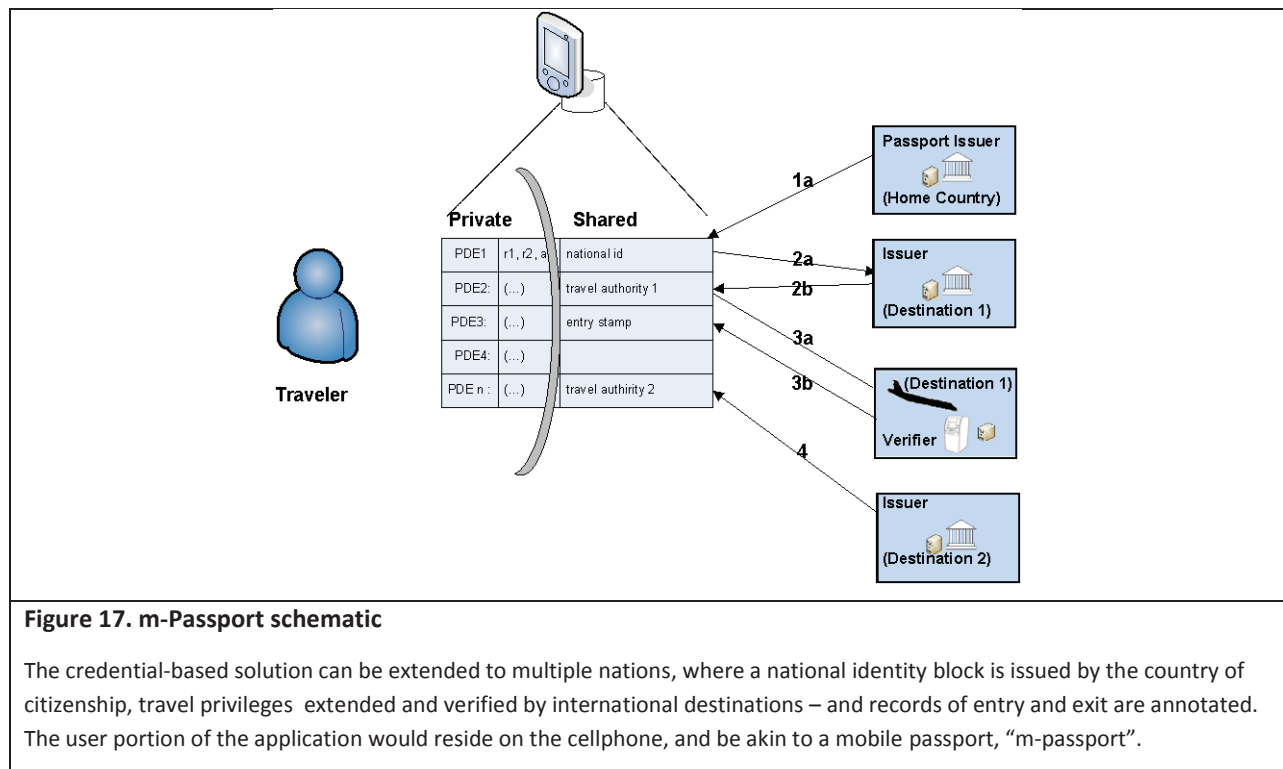
Figure 17. m-Passport schematic

The credential-based solution can be extended to multiple nations, where a national identity block is issued by the country of citizenship, travel privileges extended and verified by international destinations – and records of entry and exit are annotated. The user portion of the application would reside on the cellphone, and be akin to a mobile passport, "m-passport".

Passport may be Optional after First Verification

A special feature of the protocol presented in this report is that the e-passport may be optional after the traveller's identity has been verified. We note that biometric enrolment at the time of b-TA issuance occurs in an uncontrolled environment: no Government representative is with the traveller when the smartphone application captures and submits the fingerprint RBR and passport information. Biometric spoofing might be attempted at the time of b-TA application. The first time that physical controls are present and that biometric capture occurs in a controlled environment is when the traveller arrives in the country of destination. It is at this point that verification of the triangular binding in Figure 16 occurs. In fact, this triangular verification may only be necessary upon first-time verification: it may be possible in subsequent verifications to omit verifying the e-Passport.

Upon a first arrival the kiosk must establish biometric ownership of both the b-TA and the e-Passport, as well as the cross reference between these two. Once the complete verification has been performed, the traveller's identity becomes "verified". It is no longer an "assumed" identity. Further verification of the e-passport may be optional. The verifier may update a credential in the smartphone (which is within the scope of an m-passport study) and update the database entry.
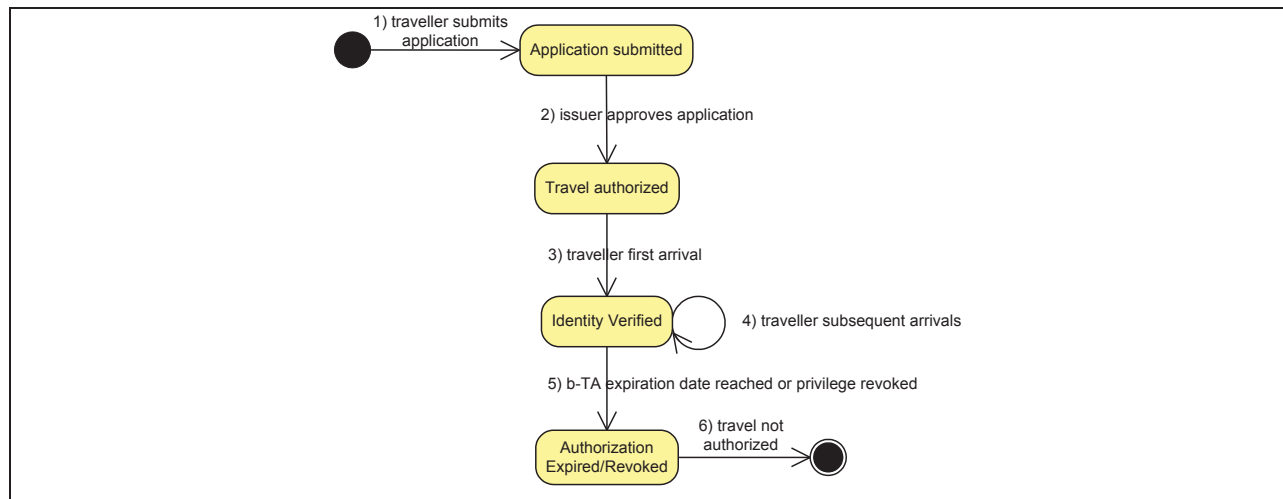
Figure 18. b-TA lifecycle

The b-TA goes through 4 major steps in its lifecycle – application, issuance, initial verification, sub-sequent use, and revocation or expiration. Once first arrival verifies identity, e-passport verification may become optional until the b-TA expires or is revoked.
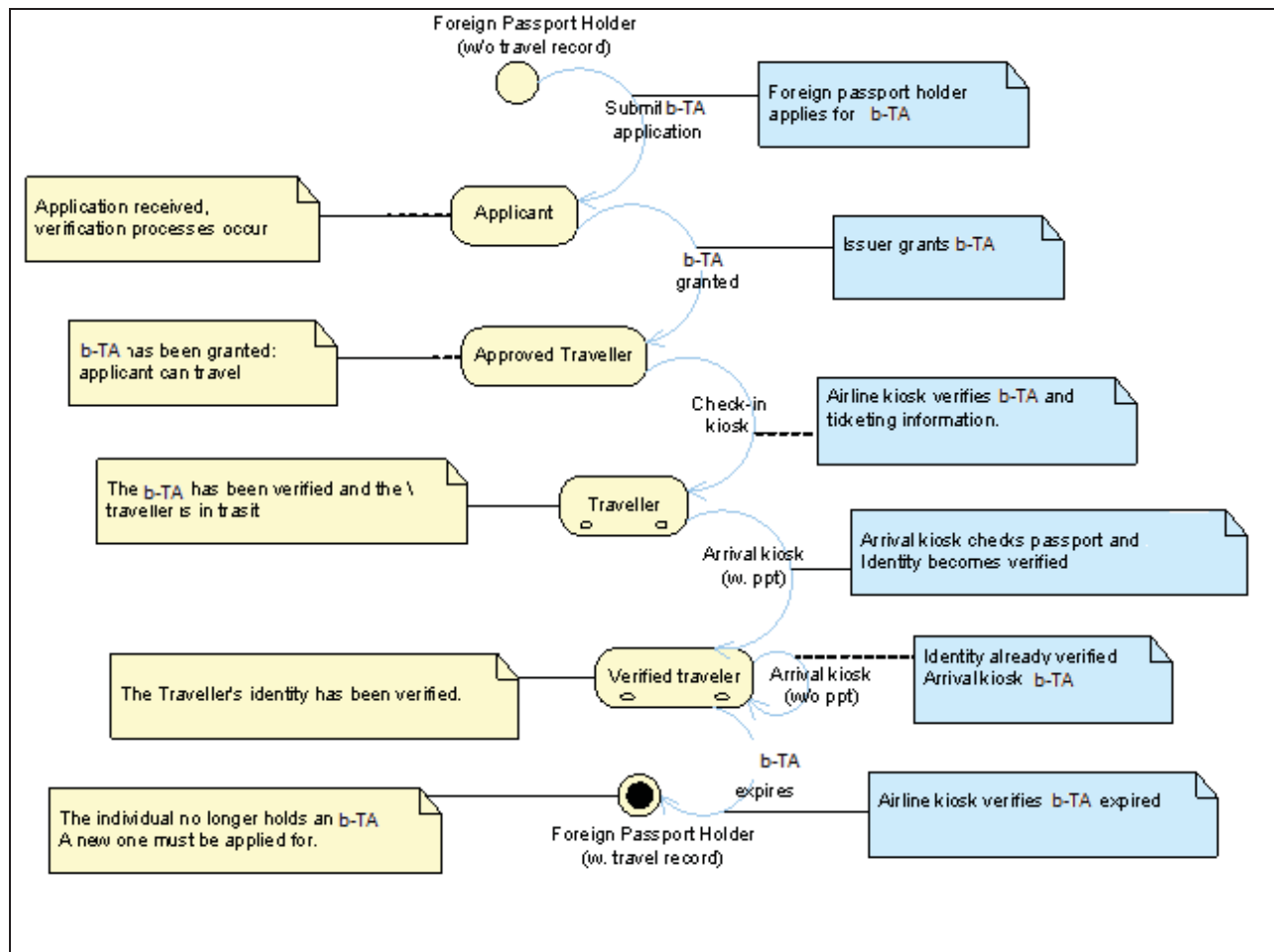
Figure 19. Traveller lifecycle.

Lifecycle of the traveller's status proceeds from an applicant to a verified traveller, to a traveller in transit, to a verified traveller again, until finally the b-TA is revoked or it expires. In the proposed approach the identity is not verified during issuance: it is a claimed identity until first verification, which occurs the first time the traveller arrives in Canada. At that time, an initial three way check occurs: individual to passport, b-TA to individual, and b-TA to passport. After this initial check, the identity is now verified and the traveller is free to continue using the b-TA during its effective period (with or without an e-passport as it may become not mandatory)

Chapter 5: Evaluation and Assessment

In this Chapter, we evaluate our proposed approach against the Security Requirements Checklist that was presented in Chapter 3. Each requirement is discussed in turn, with an evaluation and assessment provided for each requirement. The assessment indicates the readiness or level of the technology, and also serves as an indicator of future work in each area.

Security Requirements Checklist Assessment

Evaluating the proposed approach in terms of the Security Requirements from Chapter 3, we have:

Req:[1.X] **Physical security and tamper resistance**

Req:[1.1] **No data insertion and/or eavesdropping**

The system shall provide, or support the use of, suitable security mechanisms to prevent unauthorized data insertion and eavesdropping.

Eval: [1.1.1] Low current security of smartphone platforms

In evaluation of the proposed solution with respect to this requirement, we note that a smartphone equipped with a biometric sensor has been proposed as the user computer. Furthermore assumptions have been made about security of storage and integrity of executable binaries.

The security models for popular smartphone operating systems such as iOS and Android currently may not strong enough.

While there may exist technologies to monitor binary integrity or access to platform functions and data, these may be at an early stage of development and are not widely deployed or used.

Assessment: Technological Challenge

Eval: [1.1.2] Companies make it inconvenient to protect privacy

Further to the Eval: [1.1.1], it can be said that companies have low incentive to protect consumer privacy. Knowing consumer personal information and behaviours increases the effectiveness of targeted marketing campaigns, which in turn increases company revenue.

Even if the technological means are available in Eval: [1.1.1], it seems that a certain cooperation is required from the companies central to smartphone platform develoment.

Assessment: Business Challenge

Eval: [1.1.3]   Low privacy protecting mechanisms on smartphone platforms

Smartphone users are not careful about the PII they reveal. In exchange for free applications and convenience, users have allowed companies such as Google, Samsung and Apple, virtually unconstrained access to the personal data residing on their smartphones.

Even if secure technologies in Eval: [1.1.1] are available, to successfully protect user privacy, they must be used responsibly by consumers.

Assessment: User Training

Req:[1.2]   No-leakage of intermediary outputs

The system shall not permit access to the intermediate inputs or outputs of the biometric FE or PIC subsystems.

Eval: [1.2.1]   Biometrics do not leave the cellphone

The outputs of the biometric feature extractor on the smartphone are not used, nor shared with the issuer or the verifier.

Assessment: User Training

Eval: [1.2.2]   Distributed PIC: difficult to corrupt all portions

The mechanism used by the PIC is distributed throughout the system. During the *issue* protocol, the cryptographic key is generated on the cellphone and is bound with the b-TA, using the issuer's digital signature.

During the *show* protocol, a fresh biometric reference is generated and verified, using a ZKPoK.

Assessment: Good

Eval: [1.2.3]   Binary security on Smartphone

Since the key generation and reproduction occurs on the smartphone, the input of the PIC are created on a platform which, as discussed in Eval: [1.1.1], is difficult to secure. This does not jeopardize the PIC internally, but does impose a threat on its inputs.

Assessment: Further research required: security on smartphone

Req:[1.3]   No allowable blending or substitution attacks

The system shall not permit substitution or blending by an attacker or malicious insider of either the record data or any obscuring elements such as codewords, hashes, or chaff.

Eval: [1.3.1]   RBR is hidden in commitment and sealed by the

issuer's signature

We are not aware whether blending or substitution is possible. However, we note that at verification-time, biometric identity comparison occurs on a Pedersen commitment, which perfectly hides the biometrically derived key. During the *issue* protocol, the Pedersen commitment is created and further sealed into the b-TA by the issue's digital signature, which prevents tampering, and thus prevents a high level of blending or substitution attacks.

Assessment: Good

Eval: [1.3.2]   Possible weakness to smartphone security

The FE's $gen(...)$ and $rep(...)$ methods are stored on the smartphone. A mechanism should be put in place to ensure integrity of these modules.

Assessment: Further research required: Sandbox

Req:[1.4]   No leakage of raw biometric and extracted feature set

The system shall not store, transmit or emit either the raw biometric or extracted feature set (template).

Eval: [1.4.1]   No usage of biometric beyond smartphone

As in Eval: [1.2.1], this requirement is partially met with the biometric capture and FE occurring on the smartphone: these are not used for any purpose other than the generation and reproduction of RBR. The raw biometric and the biometric template are not stored, nor transmitted, nor emitted.

Assessment: Good

Eval: [1.4.2]   Possible vulnerability due to smartphone security

Proper sandbox and trust model must exist to ensure the integrity of the biometric capture and fuzzy extractor modules in the smartphone. This is an active area of R&D in industry and academia.

Assessment: Further research required: Sandbox

Req:[1.5]   No inversion of the biometrics

The system shall not output, or otherwise allow an attacker to derive, a biometric match score in such a way as to permit any attack, such as the hill-climbing attack.

Eval: [1.5.1]   Biometric inversion is protected via FE and IND-CCA2.

Reverse engineering of the biometric given the public data and cryptographic key is computationally difficult: the

PI in our system, namely R, is not stored. It is wrapped in a Pederson Commitment. The AD, namely P (helper data) is not divulged, it is encrypted in RSA OAEP.

Assessment: Good

Req:[1.6]   No inversion of keys for auxiliary data

If, in addition to providing a simple binary accept/reject record comparison decision, the system outputs a key or keys that are to be used to unlock additional cryptographically secured data, the system shall not permit the inversion of such keys, with or without the use of other available data (PI, AD) in such a way as to reveal PII.

Eval: [1.6.1]   RSA-OAEP Encryption: proven security

The system encrypts helper data P with RSA-OAEP. This is a well understood cryptosystem with proven security [BR94]..

Assessment: Good

Eval: [1.6.2]   Decryption key in secure location

The helper data encrypted by the smartphone can only be decrypted with by the CBSA verification kiosks which are located in a physically secure environment (a CBSA custom-controlled area).

Assessment: Good

Req:[1.7]   Appropriate liveness detection

If the system is to be operated without the direct oversight of authorized personnel (such as in a kiosk deployment), it shall incorporate mechanisms to mitigate biometric spoofing, such as some forms of liveness detection.

Eval: [1.7.1]   Liveness detection at verification stage only

There are two transactions to be considered: b-TA issuance and verification. The traveller side of the b-TA issuance transaction operates in an unknown, unsupervised environment (the traveller's smartphone). In this scenario, it is entirely possible that biometric spoofing might occur. This spoofing would be detected at the time of verification, which in our scenario happens in a supervised and controlled environment (a CBSA controlled area).

The need to offer the enrolment in an uncontrolled area is not required. To the contrary, it is not desired: we seek to offer the traveller the convenience application from any location.

The fact that an e-passport is used on verification and that verification occurs in a controlled environment overcomes the threat of spoofing.

Assessment: Good

Req:[2.X]   **Configuration of Operating Parameters**

Req:[2.1]   Operating characteristics configurable to operational needs

The system shall provide ability to configure operation to reach FAR and FRR that are suitable to the operational needs.

Eval: [2.1.1]   Analysis deferred.

The analysis of a) operational FAR requirements and b) the achievability of that FAR by a selected fuzzy extractor algorithm have not been addressed in this study.

Assessment: Further research required: Case Study/Prototype

Req:[3.X]   **Revocability and Renewability**

Req:[3.1]   System should provide ability to revoke or cancel the credential

In the event of a partial compromise of the IdMS (or for other operational reasons such as automatic expiry) the system shall provide the ability to revoke or cancel the credential(s) of a user.

Eval: [3.1.1]   Revocability

The issuer's b-TA query system will maintain suitable status information for each issued b-TA such that it may be revoked at any time. A revoked b-TA will fail at the time of thevalidity check transaction.

Assessment: Good

Req:[3.2]   System should provide ability to renew the biometric reference

In the event of a partial compromise of the IdMS (or for other operational reasons such as automatic expiry) the system shall provide the ability to create a new, distinct, credential that is based on the same biometric or combination of biometrics without increasing privacy leakage, FAR, or FRR.

Eval: [3.2.1]   Renewability

The fuzzy extractor's $gen(b_I, r_I)$ method allows creation of a new, distinct tuple $< R, P >$ from the same biometric b_I by supplying a new value of random data input r_I. Hence a b-TA based on such an extractor may be renewed at any time by repeating the issuance and first verification (biometric ownership) transactions. Use of an indistinguishability adapter to further encrypt the public data portion of the tuple mitigates any additional PII leakage that might otherwise be associated with the record multiplicity.

Assessment: Good

Req:[4.X]   **Unlinkability/Non-distinguishability**

Req:[4.1]   No cross-database linkage

It should not be possible for the presence or absence of an individual's credential within any other biometric IdMS to be inferred from their credential within this

IdMS.

Eval: [4.1.1] No possibility for cross system linkage exists based on the RBR given computational difficulty of underlying cryptographic techniques.

The RBR scheme used outputs indistinghuishable AD and PI. Specifically, the AD emitted consists of P_e the encrypted public data from the fuzzy extractor. It is indistinguishable by the properties of RSA-OAEP. The PI emitted are the biometric key commitments CR_I and CR_S. These are indistinguishable due to the properties of Pedersen Commitments. These indistinguishability properties protect against cross system linkage on the basis of solely these elements.

Assessment: Good

Req:[4.2]   No record multiplicity attacks

It should not be possible to mount an attack on the security of the system using record multiplicity from multiple enrolments of the same credential holder, either within the same system or across multiple biometric IdMS.

Eval: [4.2.1]   The proposed protocol provides indistinguishability of helper data and RBR

Computational properties of IND-CCA2 encryption prevents multiplicity attacks. The fuzzy extractor combined with the IND-CCA2 indistinguishability adapter hides all information about the generating biometric, in the sense that the distribution of the adapted public data P_e provides indistinguishability of helper data.

Assessment: Good

Req:[5.X]   Non-Transferability

Req:[5.1]   No b-TA lending between individuals

It must not be possible for a b-TA issued to one individual to be used by another individual.

Eval: [5.1.1]   The proposed protocol prevents unauthorized lending

Lending is prevented by a combination of cryptographic techniques and the strength of the underlying biometric modality. Cryptographic techniques ensure integrity of the issued credential and the fingerprint RBR sealed within it. Biometrics ensure correctness of ownership issuance at verification-time.

Assessment: Good

Req:[6.X]   Verifiability of Issuance

Req:[6.1]   The system must allow verification of issuer authenticity

It should always be possible to verify the validity of the b-TA by confirming it was actually issued by the issuer from whom it is claimed to be. Authenticity of the b-TA would not be verifiable if this were not achievable.

Eval: [6.1.1]   Issuer signature on credential provides verifiable authenticity

The issuer provides a digital signature on the credential. This signature is verified during the *show* protocol at which point, authenticity is confirmed, as well as integrity of the digital credential.

Assessment: Good

Req:[7.X]   Effective data based expiration of b-TAs

Req:[7.1]   Issued b-TA should have an expiration date after which they can no longer be used.

Eval: [7.1.1]   The proposed system provides expiration dates

We propose to include both Issue Date and Expiry Date attributes within the signed b-TA document. The show protocol uses the statement of proof mechanism for the underlying credential system [Bra00] to determine expiry status.

Assessment: Good

Req:[8.X]   Biometric Irreversibility

Req:[8.1]   If biometrics is used, it should not be possible to reverse engineer the biometric, given the data exchanged or stored at any point during the process.

Eval: [8.1.1]   Designed Irreversibility

Subject to the properties of the fuzzy extractor scheme adopted, as well as the encryption used, the construction provides irreversibility.

Assessment: Good

Req:[9.X]   Anonymity: [Not required]

Req:[9.1]   It is not necessary that application and passage transactions be anonymous.

Eval: [9.1.1]   Not designed for anonymity

Transactions, involving traveller application for b-TA, airline verification of issued b-TA, and CBSA verification of traveller passage, have not been designed for traveller anonymity.

Assessment: Not required

Req:[10.X]   Selective show of attributes

Req:[10.1] It is desirable for the traveller to be able to selectively show (or retain) attributes used in the b-TA.

Eval: [10.1.1]   Selective show is an embedded feature of the

presented protocols

The protocol presented in this paper is based on digital credentials, which supports selective showing of protocols. The scenario presented in this protocol has assumed that selective show between issuer and verifier is not required

Assessment: Not required[11]

---

[11] Although not necessarily required in a single country scenario, selective showing becomes fundamentally important in a multi-nation scenario.

Chapter 6: Conclusions

We have described a promising application of privacy enhancing techniques as applied to biometrics in the context of a secure electronic document suitable for use as mobile biometric-enabled electronic travel authority (b-TA) for foreign passport holders wishing to visit Canada. We have developed this scenario in detail, identifying the participating entities, transactions, and data interchanges required over the lifecycle of the document from issuance through validation, usage, and on to expiry. Based on the limitations identified in Chapter 5, we estimate that we are approximately 4-6 years from a functional system.

We identified a number of potential system vulnerabilities, and based on these, we constructed a checklist of security requirements to be met by any implementation, in order for it to be considered suitable for deployment. With this evaluation framework in place, we then presented our selected approach, provided an assessment. In a nutshell:

A) Our proposed architecture includes:

1. A biometrically secured electronic travel authority (b-TA)
2. A traveller smartphone having an installed user-application and fingerprint sensor
3. A user-application on the cellphone which:
    3.1. Coordinates the b-TA issuance, airline check in and customs-arrival processes
    3.2. Implements cryptographic protocols for privacy and security
    3.3. interfaces with the programming model of the fingerprint sensor
4. Integral touchpoints and progressive processing and mitigation of risk throughout traveller continuum:
    4.1. User convenience upon b-TA application
    4.2. Verification of authority to travel pre-boarding
    4.3. Verification of identity and document integrity at arrival
    4.4. Ability to reconcile entry-exit

B) Our proposed algorithm includes:

1. - Fuzzy extractors (aka "Biometric Encryption") running on a smartphone are suggested for privacy protection;
2. - Additional layers of encryption: Helper data are further encrypted (by RSA-OAEP) and stored on smartphone; Pedersen commitment is stored by Issuer for future validation of e-TA;
3. - The decryption key is not stored on the smartphone;
4. - Hardware protection against tampering of the information stored on the smartphone;
5. - Verification in a secure environment at a CBSA kiosk rather than on the smartphone.

As a result, of the algorithm most known attacks against fuzzy extractors are thwarted. Given the architecture and approach selected, if everything works as expected we expect this approach will enhance the system security, as well as the travellers privacy and convenience resulting in a triple-win: all the hallmarks of Privacy by Design.

Further research

This section identifies areas for future work. We believe the items would best achieved by a team including representatives from Government, Academia and Industry to most effectively leverage the strengths of each.

m-Passport application

Entirely paperless passports may be enabled by the technologies presented in this study. Further study to look at the b-TA application as a multi-nation system, includes the concept of electronic identification records for citizens. Preliminary discussion has occurred with FRONTEX. There may also be interest with IATA and ICAO in this passport technology.

Smartphone security

Further work is required to demonstrate that available smartphones can implement the RBR generation algorithms securely, particularly in relation to:

- assurance of integrity of program modules
- secure storage of personal data
- effective PETs to inform users of application access to data and platform functions
- user training

Biometric classification error performance

It will be necessary to demonstrate that the underlying biometric system can operate at a suitably low error rate. In particular, for operational security it is essential to keep a suitably low FAR while keeping a low enough FRR to benefit from any kiosk-based transactions.

Proof of concept

Device-based: A proof of concept on a representative device should be implemented. This would verify the ability to add RBR generation mechanism to a device borne sensor and do template extraction and RBR generation on the phone. As well, this would provide an initial assessment of the impact of a proof of knowledge operation on user response time.

Test data-based: It may also be valuable to implement the RBR generation mechanism on a test set of fingerprints. This would allow data analysis to be conducted for indistinguishability, irreversibility, key sizes etc.

Other applications on the traveler continuum

Although we focus on a single scenario in this report, we can envisage other applications of such secure biometric technologies within the traveler continuum Figure 20. These include b-TA application and verification for foreign nationals, trusted traveller programmes, streamlined airport passage including biometric verification by other government agencies and biometrically-enabled entry-exit recording.
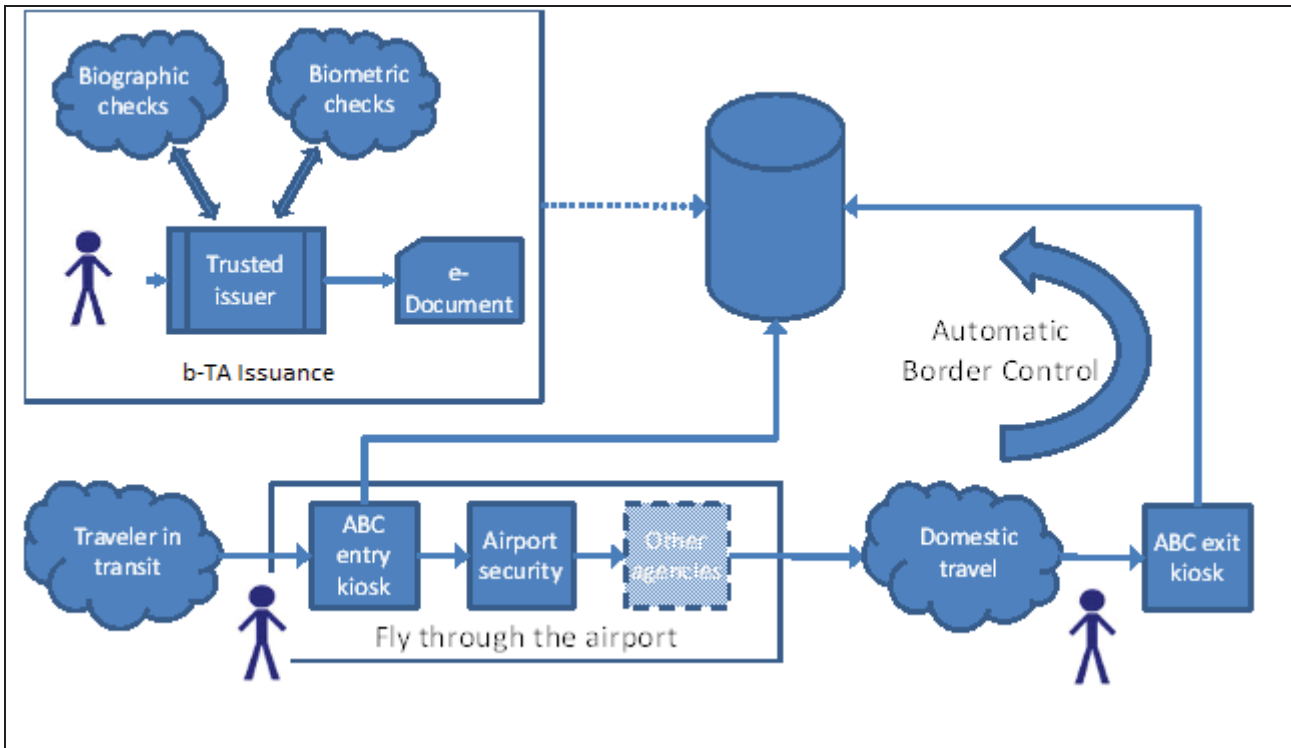

Figure 20. Integrated RBR scenario.

RBR enabled systems allow biometric verification of travellers in differing scenarios such as b-TA, Trusted Traveller, Fly-Through-the-Airport, and Entry/Exit. These scenarios can be integrated with possible overall synergies.

Key features of our approach

Convenient, low-effort initial enrolment

By developing our solution around the traveler's own smartphone device, we have increased convenience to the traveller and have reduced the human effort associated with initial b-TA enrolment. Unlike a traditional Visa issuance, b-TA enrolment does not require face-to-face interaction with a consular official of the issuing authority and, may be performed in a suitably secured online transaction requiring only biographic and perhaps civil registry information.

Secure, biometric-based binding between document and identity

Our scheme allows the b-TA to be bound securely to the traveller via biometrics by piggy-backing off the traveller's ICAO electronic passport (e-passport). This in turn allows the possibility of using the validated b-TA as a primary travel document either by choice or in the case of loss or expiry of the original e-passport.

Cryptographically strong hiding of PII

We believe that our proposed solution intrinsically provides good protection of PII, going beyond the ISO 24745 recommendation by adding a layer of encryption (INDCCA2 indistinguishability) and hiding (Pedersen commitment) to the basic ISO RBR.

Good emerging standards support

By aligning with ISO 24745 Model G (*store distributed on token and server, compare on server*), we delegate control of the biometrically-derived portion of the RBR back to the user, giving an extra layer of assurance that the user's biometric cannot be obtained (even in cryptographically secured form) by compromise of the IdMS database.

We believe that these assurances will aid both end-user acceptance and conformance with international regulatory requirements (in particular EU privacy and data protection laws).

Challenges for implementation and adoption

Security of the available smartphone hardware and operating systems

The NIST Level-4 security specification requires FIPS 140-2 Level 2 compliance of any cryptographic module. While FIPS 140-2 Level 2 permits the use of general purpose computing devices and unevaluated operating systems [FIPS140-2], it does impose requirements on tamper-proofing or tamper-evidencing, which may not be met by currently available devices. As well as physical security, we need to be assured of electronic security – in particular that any third-party cryptographic libraries are secure, and that software and firmware updates are

handled securely. Not all smartphones currently provide biometric functionality, and for those that do it is not clear that the currently available smartphones provide sufficient physical and electronic security[12].

While niche applications such as the b-TA may help drive development of suitably secure biometric-enabled devices, it will likely require a much more general uptake of biometric-based IdMS systems to provide strong commercial justification.

Good privacy practices may be inconvenient

Users are sometimes tempted to turn off or disable security features if they are perceived to interfere with normal device usage. Providing high security for applications on a general purpose device such as a smartphone requires a sophisticated trust model that satisfies the interests of multiple parties (end user, content provider, device manufacturer).

Smartphone users may not be careful about the PII they reveal

Delegating storage of the b-TA to the user's smartphone device is good from the point of view of giving absolute control of their PII, but it also delegates responsibility for that storage. Some user education may be required to encourage users to treat the security of their e-documents as carefully as that of a physical travel document.

---

[12] There has been at least one claim to have defeated Apple's iPhone 5S *Touch ID* system by means of a high-resolution photograph of a fingerprint [http://news.cnet.com/8301-13579_3-57604067-37/hackers-claim-to-have-defeated-apples-touch-id-print-sensor/ retrieved 20th March 2014]

Appendix 1: Abbreviations

AC-OT	Oblivious transfer with access control
AD	Auxiliary Data
AID	Application specific identifier
b	An input string
b'	Another input string
BE	Biometric Encryption
BR	Biometric Record
BSI	Blended Substitution Attack
C	Credential
CBSA	Canada Border Services Agency
CBP	US Customs Border Protection
CI	Common Identifier
CIC	Citizenship and Immigration Canada
CoP	Community of Practice
DET	Decision Error Trade-off
DRDC	Defence research and development Canada
ECC	Error Correcting Code
e-document	Electronic document
e-passport	Electronic passport
eTA	Electronic Travel Authority (Existing CIC Programme)
ESTA	Electronic System for Travel Authorization (US CBP)
b-TA	mobile biometric electronic Travel Authority (proposed approach under this document)
EU	European Union
FAR	False Accept Rate
FCS	Fuzzy Commitment Scheme
FE	Feature Extraction
FMR	False Match Rate
FNMR	False Non-Match Rate
FP7	Seventh framework programme
FRONTEX	"frontières extérieures" *(Agency for the Management of Operational Cooperation at the External Borders of the European Union)
FRR	False Reject Rate
FVS	Fuzzy Vault Scheme
GmBH	Gesellschaft mit beschränkter Haftung, German for "companies with limited liability"
I	Issuing Organization
IATA	International Air Transport Association
IBG	International Biometrics Group
IBM	International Business Machines Corporation
IdMS	Identity Management System
IND-CCA2	Indistinguishability under adaptive chosen ciphertext attack

IR	Identity Reference
ISO	International Organization for Standardization
IUPUI	Indiana University Purdue University Indianapolis (pg 12)
m-passport	mobile passport
NIST	National Institute of standards and technology
P	Prover (pg 13 - Proof of Knowledge)
P	Helper data (pg 13 - Secure sketches and fuzzy extractors)
PET	Privacy Enhancing Technologies
PI	Pseudonymous Identifier
PIC	Pseudonymous Identifier Comparator
PII	Personally Identifiable Information
PIR	Pseudonymous Identifier Recorder
PoK	Proof of Knowledge
PPB	Perfectly Private Biometric
PPBE	Perfectly Private Biometric Encryption
PRIME	Privacy and Identity Management for Europe
PSTP	Public Security Technical Program
QIM	Quantized Index Modulation
R	Random String
RBR	renewable biometric reference
RCMP	Royal Canadian Mounted Police
RSA	A cryptosystem, which is designed by Ron Rivest, Adi Shamir, and Leonard Adleman
RSA-OAEP	RSA encryption with Optimal Asymmetric Encryption Padding
SAR	Successful attack rate
SAP	A German multinational software corporation
SKI	Surreptitious Key-Inversion Attack
TC	Transport Canada
TRL	Technology Readiness Level
TURBINE	Trusted Revocable Biometric Identities
U	User
U of T	University of Toronto
UUID	Unique User Identifier
V	Verifier
WP2	Work Package 2
X	Credential attributes
ZKPoK	Zero knowledge Proof of knowledge

References

[ABC4Trust]   ABC4Trust Project Webpage
               https://abc4trust.eu/
               (Accessed 29 July, 2014)

[Ada11]   C. Adams, "Achieving non–transferability in credential systems using
               hidden biometrics." Security and Communication Networks 4, no. 2 (2011):
               195-206.

[Adl04]   A. Adler, "Images can be regenerated from quantized biometric match
               score data." In Electrical and Computer Engineering, 2004. Canadian
               Conference on, vol. 1, pp. 469-472. IEEE, 2004.

[AU4EU]   AU4EU website
               http://www.au2eu.eu/about-au2eu.html
               (Accessed 29 July, 2014)

[Bal08]   L. Ballard, et al. "Towards practical biometric key generation with
               randomized biometric templates." Proceedings of the 15th ACM
               conference on Computer and communications security. ACM, 2008.

[Bis13]   D. Bissessar, Cryptographic Credentials with Privacy-preserving Biometric
               Bindings. Diss. University of Ottawa, 2013.

[Bis14]   D. Bissessar et al., "Using Biometric Key Commitments to Prevent
               Unauthorized Lending of Cryptographic Credentials" submitted for
               publication

[Boy04]   X. Boyen, "Reusable cryptographic fuzzy extractors." Proceedings of the
               11th ACM conference on Computer and communications security. ACM,
               2004.

[BR94]   Optimal Asymmetric Encryption – How to Encrypt with RSA. Mihir Bellare
               and Phillip Rogaway. EUROCRYPT '94, LNCS vol. 950, pp. 341-358, Springer,
               1995

[Bra00]   S. Brands, "Brands, Rethinking Public Key Infrastructures and Digital
               Certificates." (2000).

[Bri07]   Bringer, Julien, Hervé Chabanne, Gérard Cohen, Bruno Kindarji, and Gilles
               Zémor. "Optimal iris fuzzy sketches." In Biometrics: Theory, Applications,
               and Systems, 2007. BTAS 2007. First IEEE International Conference on, pp.

1-6. IEEE, 2007.

[BSW07]   T.E. Boult, , Scheirer W.J., R. Woodworth, "Revocable fingerprint
               biotokens: accuracy and security analysis" in Proc. IEEE Inter. Conf. on
               Comput. Vis. and Patt. Recog, USA, 2007

[Bund11]   BioKeyS III-Final Report; "Study of the Privacy and Accuracy of the Fuzzy
               Commitment Scheme"; Bundesamt für Sicherheit in der
               Informationstechnik, 2011

[Can07]   R, Canetti, et al. "Nontransferable anonymous credentials." U.S. Patent
               7,222,362, issued May 22, 2007.

[CBP2014]   CBP ESTA Webpage
               http://www.cbp.gov/travel/international-visitors/esta
               (accessed March 28, 2014)

[CDN10b]   J. Camenisch, et al. "Unlinkable Priced Oblivious Transfer with
               Rechargeable Wallets," in Proc. of the 14th International Conference on
               Financial Cryptography and Data Security (FC 2010)

[CE86]   D. Chaum, and J-H. Evertse. A secure and privacy-protecting protocol for
               transmitting personal information between organizations. In CRYPTO '86,
               vol. 263 of LNCS, pp. 118-167. Springer-Verlag, 1987

[Cha06]   W. Chang, R. Shen, and F. W. Teo, "Finding the Original Point Set Hidden
               Among Chaff," in ASIACCS '06: Proc ACM Symp Information, Computer And
               Communications Security. 2006, pp. 182–188, ACM.

[Cha85]   D. Chaum, Security without identication: Transaction systems to make big
               brother obsolete. Communications of the ACM, 28(10):1030-1044, 1985.

[Che96]   L. Chen, "Access with pseudonyms." Cryptography: Policy and Algorithms.
               Springer Berlin Heidelberg, 1996.

[CIC2014]   CIC eTA Webpage
               http://www.cic.gc.ca/english/department/acts-regulations/forward-
               regulatory-plan/eta.asp
               (accessed March 28, 2014)

[CL01] J. Camenisch, and A Lysyanskaya. "An efficient system for non-transferable anonymous credentials with optional anonymity revocation." Advances in CryptologyEUROCRYPT 2001 (2001): 93-118.

[CKL03] Clancy, T. Charles, Negar Kiyavash, and Dennis J. Lin. "Secure smartcardbased fingerprint authentication." In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pp. 45-52. ACM, 2003.

[CP92] D. Chaum, and T. P. Pedersen, "Wallet databases with observers." Advances in Cryptology—CRYPTO'92. Springer Berlin Heidelberg, 1993.

[CS09] Cavoukian, A. and Stoianov, A. (2009) Biometric Encryption: The New Breed of Untraceable Biometrics, in Biometrics: Theory, Methods, and Applications (eds N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou), John Wiley & Sons, Inc., Hoboken, NJ, USA.
doi: 10.1002/9780470522356.ch26

[CST06] Chang, Ee-Chien, Ren Shen, and Francis Weijian Teo. "Finding the original point set hidden among chaff." Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ACM, 2006.

[Dam88] I. Damgård, "Payment systems and credential mechanisms with provable security against abuse by individuals." In Advances in Cryptology CRYPTO88, pp. 328-335. Springer Berlin/Heidelberg, 1990.

[Dam99] Damgård, Ivan. "Commitment schemes and zero-knowledge protocols." Lectures on Data Security (1999): 63-86.

[DFM98] Davida, George I., Yair Frankel, and Brian J. Matt. "On enabling secure applications through off-line biometric identification." In *Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on*, pp. 148-157. IEEE, 1998.

[DRS04] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." Advances in cryptology-Eurocrypt 2004. Springer Berlin Heidelberg, 2004

| [DRS08] | Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy Extractors--A Brief Survey of Results from 2004 to 2006." (2008). |

| [PSTP351] | Biometric Data Safeguarding Technologies Analysis and Best Practices. Gorodnichy D., Bissessar, D. Du, Y. Thieme, M. Moore, Kim, Hart; Corporate author(s): Defence R&D Canada - Centre for Security Science, Ottawa ONT (CAN) |

| [FIPS140-2] | FIPS PUB 140-2 Security Requirements for Cryptographic Modules; May 25, 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf%E2%80%8E (accessed 09/01/2014) |

| [FRONTEX2014] | Development of Capabilites for Passenger Analysis Units, Operational Heads of Airports Conference 2014 Warsaw, 04 – 07 February 2014 |

| [Gol01] | Goldreich, Oded. "Foundations of Cryptography: Basic Tools, Volume 1. Cambridge University Press, New York, NY, 2001. |

| [Gol04] | Goldreich, Oded. "Foundations of Cryptography: Basic Applications, Volume 2. Cambridge University Press, New York, NY, 2004. |

| [HAD06] | Hao, Feng, Ross Anderson, and John Daugman. "Combining crypto with biometrics effectively." *Computers, IEEE Transactions on* 55, no. 9 (2006): 1081-1088. |

| [ICAO9303] | Doc, I. C. A. O. 9303-machine readable travel documents-part 1-2. Technical report, International Civil Aviation Organization, 2006, 2006. |

| [IDEMIX] | IBM Identity Governance web page http://www.zurich.ibm.com/security/idemix/ (accessed 09/01/2014) |

| [ISO10] | ISO/IEC 24787:2010 Information technology -- Identification cards -- On-card biometric comparison |

| [ISO11] | Information Technology - Security techniques - Biometric Information Protection, ISO/IEC IS 24745, June 2011. |

[ISO13] Traveler processes for biometric recognition in automated border control systems, ISO/IEC JTC 1/SC 37 N5589, July 2013

[ISO13b] Information Technology — ISO/IEC WD 30136 — Performance Testing of Template Protection Schemes, ISO/IEC JTC 1/SC 37 N 5619, August 2013

[JS02] Juels, A., M. Sudan,: A Fuzzy Vault Scheme. In: IEEE International Symposium on Information Theory (2002)

[JW99] Juels, Ari, and Martin Wattenberg. "A fuzzy commitment scheme." In Proceedings of the 6th ACM conference on Computer and communications security, pp. 28-36. ACM, 1999.

[Kan08] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris". In BSYM '08, Tampa, FL. Pp. 59-64, 2008.

[Kev05] Kevenaar, Tom AM, et al. "Face recognition with renewable and privacy preserving binary templates." Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on. IEEE, 2005.

[LRSW99] Lysyanskaya, Anna, Ronald Rivest, Amit Sahai, and Stefan Wolf. "Pseudonym systems." In Selected Areas in Cryptography, pp. 184-199. Springer Berlin/Heidelberg, 2000.

[LT03] Linnartz J.-P., and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates." In 4th Int. Conf. on Audio and Video Based Biometric Person Authentication, pp. 393– 402, Guildford, UK, 2003.

[Luc08] Ballard, Lucas, et al. "Towards practical biometric key generation with randomized biometric templates." Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008.

[NIST11] William E. Burr et al., Special Publication 800-63-1 Electronic Authentication Guideline, NIST December 2011

[NNJ08] Nagar, Abhishek, Karthik Nandakumar, and Anil K. Jain. "Securing fingerprint template: Fuzzy vault with minutiae descriptors." In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pp. 1-4.

IEEE, 2008.

[OMB M-04-04]   Office of Management and Budget, E-Authentication Guidance for Federal
                 Agencies (OMB Memorandum M-04-04) (Dec. 16, 2003)
                 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
                 accessed 12/23/2013

[Primelife]   Prime Life website (part of European Union 7th Framework Project)
                 http://www.primelife.eu
                 (accessed 12/23/2013)

[Ped92]   Pedersen, Torben. "Non-interactive and information-theoretic secure
                 verifiable secret sharing." In Advances in Cryptology—CRYPTO'91, pp. 129-
                 140. Springer Berlin/Heidelberg, 1992.

[RU11]   Rathgeb, Christian, and Andreas Uhl. "A survey on biometric cryptosystems
                 and cancelable biometrics." EURASIP Journal on Information Security
                 2011.1 (2011): 1-25.

[SAM11]   Pierangela Samarati (Ed.), Final report on mechanisms, Privacy and Identity
                 Management in Europe for Life D2.4.1, May 2011

[Sav04]   Savvides, Marios, BVK Vijaya Kumar, and Pradeep K. Khosla. "Cancelable
                 biometric filters for face recognition." Pattern Recognition, 2004. ICPR
                 2004. Proceedings of the 17th International Conference on. Vol. 3. IEEE,
                 2004.

[SB07]   Scheirer, Walter J., and Terrance E. Boult. "Cracking fuzzy vaults and
                 biometric encryption." *Biometrics Symposium, 2007*. IEEE, 2007.

[SKTP09]   Simoens, Koen. Pim Tuyls, and Bard Preneel. "Privacy weaknesses in
                 biometric sketches." In Security and Privacy, 2009 30th IEEE symposium
                 on, pp. 188-203. IEEE, 2009.

[Sou98]   Colin Soutar ; Danny Roberge ; Alex Stoianov ; Rene Gilroy and Bhagavatula
                 Vijaya Kumar "Biometric Encryption using image processing", Proc. SPIE
                 3314, Optical Security and Counterfeit Deterrence Techniques II, 178 (April
                 1, 1998)

[SP 800-63-1] Burr, William E., et al. SP 800-63-1. Electronic Authentication Guideline. (2011).

[Stastna2014] Malaysia Airlines affair raises security concerns over passport trafficking
http://www.cbc.ca/news/world/malaysia-airlines-affair-raises-security-concerns-over-passport-trafficking-1.2568491

[Sto09] Stoianov, A., T. Kevenaar, and M. Van der Veen. "Security issues of biometric encryption." *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference*. IEEE, 2009.

[Sto10] Stoianov, Alex. "Cryptographically secure biometrics." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2010.

[Sut09] Sutcu, Yagiz, Qiming Li, and Nasir Memon. "Design and analysis of fuzzy extractors for faces." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2009.

[URPOVE] Microsoft research U-Prove web page
http://research.microsoft.com/en-us/projects/u-prove/
(accessed 09/01/2014)

[USJ05] Uludag, Umut, Sharath Pankanti, and Anil K. Jain. "Fuzzy vault for fingerprints." *Audio-and Video-Based Biometric Person Authentication*. Springer Berlin Heidelberg, 2005.

[Van06] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and Fei Zuo, "Face Biometrics with Renewable Templates". Proc. SPIE, v. 6072, 2006

[Zoy2014] Zozaya, Ignacio (FRONTEX) Personal communication with D. Bissessar, CBSA (February, March, 2014).